Maîtrise de mathématiques (MAlg 1), 2003/2004 module MAlg 1 "Algèbre" (=Master 1, MAT 401i)

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

Mon cours porte sur les fondements algébriques necéssaires pour la poursuite d'études en DESS "Cryptologie, Sécurité et Codage d'Information" (mais aussi souhaitables pour DEA, dans la géométrie algébrique et la théorie des nombres).

Il s'agit premièrement des outils d'algèbre commutative : *anneaux, corps, polynômes* utilisés en
- théorie des codes-correcteurs d'erreurs
- cryptologie à clef publique.

Il existe une analogie profonde entre l'ensemble $\mathbb{Z}$ des nombres entiers et l'ensemble des polynômes $\mathbb{Q}[x]$ à coefficients dans l'ensemble $\mathbb{Q}$ des nombres rationnels (ou l'ensemble des polynômes $\mathbb{K}[x]$ à coefficients dans un corps $\mathbb{K}$). En effet, tous les deux ensembles sont des *anneaux* avec une division euclidienne (division avec reste).

Il est utile d'étudier la divisibilité des polynômes de point de vue de divisibité des nombres, et réciproquement, on expliquera dans le cours comment on peut voir les nombres comme un analogue des fonctions. Dans le cours on développe systematiquement cette analogie : *le théorème chinois des restes* est analogue au *théorème de l'interpolation de Lagrange*, ce que permet d'effectuer *la multiplication rapide des polynômes*. Les *polynômes irréductibles* sont analogues des *nombres premiers*. *La théorie des corps finis* est entièrement basée sur cette analogie.

Vers la fin du cours on considère les systèmes algébriques sur $\mathbb{Z}$ ou sur un corps fini vus comme des *variétés algébriques*.

*Un cours dans le cadre de Master-1

Table des matières

Programme du module MAlg 1 "Algèbre"

I) Arithmetique élémentaire
- Divisibilité des entiers, pgcd, ppcm, congruences
- Entiers modulo n, Théorème de résidus chinois
- $\mathbb{Z}/p\mathbb{Z}$ est un corps, petit théorème de Fermat
- Carrés dans $\mathbb{Z}/p\mathbb{Z}$, symbole de Legendre, lois de réciprocité de Gauss

II) Corps finis et polynômes
- Rappels sur la notion de corps, exemples
- Division euclidienne dans $\mathbb{K}[x]$, racines d'un polynôme, formule d'interpolation de Lagrange
- Polynômes irréductibles, extensions, degré, corps de rupture
- Sous-groupes finis dans $\mathbb{K}^*$
- Frobenius, structure des corps finis
- Algorithme de factorisation de Berlekamp dans $\mathbb{F}_p[x]$

III) Equations algébriques et variétés affines
- Solution d'un système linéaire sur les anneaux et Théorème de Bezout
- Solution d'un système algébrique et homomorphismes d'anneaux
- Variétés affines (exemples). Courbes planes, points singuliers

Si le temps le permet :
- Cubiques planes, lois de groupe, points rationnels sur des exemples

Prérequis : Le cours est accessible aux étudiants de Master 1 en Mathématiques et en Mathématiques Appliquées. Tous les résultats des cours d'algèbres de L3 de mathématiques utilisés serons révisés. Le cours se constitut un minimum en algèbre et en théorie des nombres indispensable pour continuer des études en M2.

Remarque : Nouveaux éléments par rapport aux cours d'algèbre de L3 :

- *aspects algorithmiques des opérations algébriques*
- *bases algébriques pour :*
  - cryptographie à clef publique
  - théorie des codes–correcteurs d'erreurs
- *Analogies entre les nombres et les polynômes. Equations algébriques et variétés affines.*

Cours N°1. Jeudi le 2 octobre 2003

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

1 Les entiers

1.1 Divisibilité des entiers. Lien avec l'algèbre et l'analyse.

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 $\sharp X$ son cardinal :

$$\sharp X = \mathrm{Card}\,(X) = |X|.$$

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 la 19 siècle).

DÉFINITION 1.1.1 *Si a et b sont deux entiers relatifs , on dit que a* divise *b et on note $a|b$ s'il existe un entier relatif c tel que $b = ac$. On dit également que b est un* multiple *de a ou a un* diviseur *de b. On note $a\mathbb{Z}$ l'insemble des multiples de a.*

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.
Un nombre entier positif n est dit composé *s'il n'est pas premier.*

Par exemple, $2 \mid 6$ et $389 \mid 97734562907$:

$$97734562907 = 389 \cdot 251245663 = 41 \cdot 193 \cdot 389 \cdot 31751.$$

Les nombres premiers sont

$$2, 3, 5, 7, 11, \ldots, 41, \ldots, 193 \ldots, 389, \ldots, 2003, \ldots, 31751, \ldots.$$

et les nombres composés sont

$$4, 6, 8, 9, 10, 12, \ldots, 666 = 2 \cdot 3^2 \cdot 37, \ldots, 2001 = 3 \cdot 23 \cdot 29, \ldots.$$

(voir [Stein], Chap. 1).

Maintenant supposons que n est tout entier positif. Alors, de même façon, n peut être écris comme un produit des nombres premiers :

– Si n est premier, c'est fait.
– Si n est composé alors $n = ab$ avec $a, b < n$.

En utilisant raisonnement par récurrence, a, b sont tous les deux produits des nombres premiers, donc n est aussi un produit des nombres premiers. Ce résultat explique le terme *nombre premier* : tous les autres entiers positives sont construites commes leurs produits.

Deux résultats de base de la théorie des nombres

(connues des cours de licence) disent :

(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

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

Le premier résultat se demontre par l'absurde : si l'on avait $\mathcal{P} = \{p_1, p_2, \cdots, p_n\}$, on considèrera $q = 1 + p_1 p_2 \cdot \ldots \cdot p_n$. Alors, $q \notin \mathcal{P}$ par l'hypothèse, mais aucun p_i divise q, contradiction avec ce qui précède.

On rapellera une démonstration du deuxième resultat plus tard, sous une forme plus générale (pour tous les anneaux eucildiens).

Rappelons quelques propriétés de base de la divisibilité :

Proposition 1.1.2 *Si a, b, c sont des entiers relatifs, on a*
(i) $a|a$
(ii) si $a|b$ et $b|c$, alors $a|c$
iii) si $a|b$ et $a|c$, alors $a|b+c$

Définition 1.1.3 *Si b et un entier relatif non nul,et si a et un entier relatif il existe une unique paire (q, r) d'entier relatifs tels que $a = bq + r$ avec $0 \leq r < |b|$. L'entier q est appelé le quotient de a par b, et r le reste de la division, on le notera ici $a\%b$ (ou $a \bmod b$).*

Exercice 1.1.4 *Démontrer en détails Proposition 1.1.2*

Lien avec l'algèbre et l'analyse. Analogies entre nombres et fonctions.

L'exsemble $\mathbb{Z}$ est un *anneau commutatif* : il existe deux opératons suivantes : pour tous paires $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ on a

$$+ : \mathbb{Z} \times \mathbb{Z}, (a, b) \mapsto c = a + b \in \mathbb{Z} \quad (\text{"}addition\text{"});$$
$$\times : \mathbb{Z} \times \mathbb{Z}, (a, b) \mapsto d = a \times b = a \cdot b \in \mathbb{Z} \quad (\text{"}multiplication\text{"});$$

avec les propriétés des axioms d'anneaux (commutativité et associativité de $+$ et de $\times$, distributivité $a(b_1 + b_2) = ab_1 + ab_2$, l'existence de 0 et de 1, l'existence d'un (unique) élémént opposé $-a \in \mathbb{Z}$ à tout $a \in \mathbb{Z}$.

L'anneau des nombres entiers $\mathbb{Z}$ est un objet algébrique fondamental, aussi bien que l'anneau $\mathbb{R}[X]$ ($\mathbb{C}[X]$) des polynômes à coefficients réels (complexes). Ces deux anneaux sont commutatifs, associatifs unitaires sans diviseurs de zéro. Il est commode d'exprimer la notion de divisibilité dans un anneau R ci–dessus à l'aide de la notion d'*idéal :*

rappellons qu'un idéal I de R est une partie de R qui est fermée par rapport aux opérations : pour tous $a, b \in I$)

l'addition $a + b \in I$, *passage à l'opposé*, $a \mapsto -a$, et la *multiplication externe* par tout élément x de R : $a \mapsto ax$.

Tout élément $a \in R$ définit l'idéal $I = (a) = \{ax \mid x \in R\}$, et l'affirmation "$a$ divise b" est équivalent à "$b \in (a)$".

Un idéal de type (a) est appelé idéal *principal*, et on rappelera que les anneaux $R = \mathbb{Z}$, $\mathbb{R}[X]$, $\mathbb{C}[X]$ sont principaux, c'est à dire, tous ces ideaux sont *principaux*.

La démonstration de ce fait est la même pour les nombres et pour les polynômes : pour un idéal I quelconque on effectue la division avec reste par un élément non nul de I avec la plus petite valeur absolue (le plus petit degré respectivement), et la définition d'idéal implique que le reste doit être zéro.

On verra que le théorème de l'existence et de l'unicité de décomposition en facteurs irréductibles est valable dans tout anneau principal.

EXEMPLE 1.1.5 *L'unicité dans la deuxième propriété n'est pas toujours valable même si l'existence d'une décomposition en éléments premiers a lieu. Un exemple connu est donné par l'anneau* $\mathbb{Z}[\sqrt{-5}]$ *dans lequel il existe essentiellement différentes factorisations en éléments premiers :*

$$2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}).$$

EXEMPLE. PROBLÈME DE FERMAT. Pierre de Fermat (1601–1665) à soulevé son probème 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 second 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 :

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

("Fermat's Last Theorem").

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, la décomposition unique en facteurs premiers). Immédiatement J.Liouville dit : "N'y a-t-il pas là une lacune à remplir ?" (et dans quelques mois 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.

Nombres comme analogues des fonctions

L'opération de division avec reste permet de voir tout nombre entier a comme une fonction

$$f_a : \mathcal{P} \to \mathbb{N}, \quad p \mapsto a\%p = a \bmod p. \tag{1.1}$$

EXEMPLE 1.1.6

$$f_{20}(3) = 2, f_{20}(7) = 6, f_{20}(2) = 0, f_{20}(5) = 0, f_{20}(257) = 20$$
$$f_{-1}(3) = 2, f_{-1}(7) = 6, f_{-1}(2) = 1, f_{-1}(5) = 4, f_{-1}(257) = 256$$

Ceci dit, les fonctions f_{20} et f_{-1} prennent les mêmes valeurs en $p = 3$ et $p = 7$. La fonction f_{20} possède "un zéro double" en $p = 2$, car $20 = 2^2 \cdot 5$, tandis que la fonction f_{-1} n'a pas de zéros.

EXERCICE 1.1.7 *Montrer que si n est premier alors la fonction f_n ne s'annule qu'en un seul point . L' affirmation réciproque est-elle vraie ?*

EXERCICE 1.1.8 *Déssiner la fonction f_6.*

EXERCICE 1.1.9 *Montrer que tout nombre entier a est déterminé par la fonction correspondente f_a*

1.2 Factorisation des nombres. Lien avec l'informatique et l'algorithmique.

Soit $n = 1275$, et remarquons que $17 \mid 1275$, alors n est certainement composé, $n = 17 \cdot 75$. Puis, 75 est $5 \cdot 15 = 5 \cdot 5 \cdot 3$. Donc finalement, $1275 = 3 \cdot 5 \cdot 5 \cdot 17$.

Remarquer qu'on peut agir différement pour factoriser le nombre 1275, par exemple $1275 = 5 \cdot 255$. On obtient $255 = 5 \cdot 51$ et $51 = 17 \cdot 3$, donc le résultat final est le même. Le résultat sur l'unicité ci-dessus dis que c'est toujours le cas.

Lien avec l'informatique et l'algorithmique. Ecriture base $m \in \mathbb{N}$.

Pour effectuer les opérations algébriques dans $\mathbb{Z}$ on utilise un système de numération de la base $m \in \mathbf{N}$: la notation

$$d = (d_{k-1}, d_{k-2},\ ...,\ d_1, d_0)_m$$

signifie que $d = d_{k-1}m^{k-1} + ... + d_0$ avec des chiffres $d_i \in \{0, 1, ..., m-1\}$. Le nombre de chiffres d_i utilisés pour cela est égale à $[\log_m n] + 1$. Une méthode commode utilsée par les ordinateurs correspond à $m = 2$, et on appelle le système de numération binaire (de la base 2). Le chiffre (digit) binaire (c'est à dire 0 ou 1) s'appelle "bit" (en anglais "bit" est une abréviation de "binary digit").

L'analyse simple des algorithmes "scolaires" pour l'addition et pour la multiplication montre que pour l'addition de deux nombres écrits avec k et l bit, $k \geq l$, on a besoin de k operations booleénnes (bit–opérations) qui se réduisent à l'addition des chiffres correspondants, (avec mémorisation et transfert du chiffre 1 à la position précédente dans le cas "1 + 1").

EXEMPLE 1.2.1

$$\begin{array}{cccccccccc} & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 1} & & & & & \\ & 1 & 1 & 1 & 1 & 0 & 0 & 0_{(2)} & & \\ + & 0 & 0 & 1 & 1 & 1 & 1 & 0_{(2)} & & (120 + 30 = 150) \\ & - & - & - & - & - & - & - & & \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0_{(2)} & & \end{array}$$

Dans cet exemple $(1111000)_2 = 8 \cdot 15 = 120$, $(0011110)_2 = 2 \cdot 15 = 30$.

On voit que pour la multiplication des nombres à k et l chiffres on a besoin de $2kl$ bit–opérations.

Exemple 1.2.2

$$\begin{array}{cccccccccc} & & & & 1 & 1 & 0 & 1_{(2)} & & \\ \times & & & & & 1 & 1 & 1_{(2)} & & \\ - & - & - & - & - & - & - & - & - & \\ & & & & 1 & 1 & 0 & 1 & & \\ & & & 1 & 1 & 0 & 1 & & & \\ + & & 1 & 1 & 0 & 1 & & & & \\ - & - & - & - & - & - & - & - & - & \\ 1 & 0 & 1 & 1 & 0 & 1 & 1_{(2)}, & & & \end{array} \qquad (13 \times 7 = 91).$$

Le nombre de bit–opérations nécessaires pour l'exécution d'un algorithme caractérise essentiellement *le temps d'exécution.*

Passage d'un système de numération à un autre. Le temps nécessaire pour passer de la forme binaire d'un nombre n vers la forme de la base m est facile à estimer par $(k^2 l)$ car on a besoin pour cela de (k) divisions avec reste, avec pour chaque division (kl) bit–opératons ("division en colonne") où l est le nombre de bit dans l'écriture de m, k est le nombre de bit dans l'écriture de n.

Remarque. Rappelons que la *méthode de Hörner* permet de trouver facilement la valeur $n = \sum_{i=0}^{r} c_i m^i$.

On considère le polynôme

$f(x) = g_n(x) = \sum_{i=0}^{r} c_i x^i$, et $x = m$ on calcule $g_n(m)$ de façon suivante : soient

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0, \ a_n \neq 0$$

un polynôme, et on cherche un autre polynôme

$$q(x) = b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + \cdots + b_0, \quad b_{n-1} \neq 0$$

tel que

$$f(x) = (x - c) q(x) + r,$$

En comparant les coefficients des puissances de x on obtient

$$a_n = b_{n-1}, \ a_{n-2} = b_{n-2} - c b_{n-1}, \ \cdots,$$

$$a_1 = b_0 - c b_1, \ a_0 = r - c b_0, \ r = f(c).$$

Ceci implique

$$b_{n-1} = a_n, \ b_{n-k} = c b_{n-k+1} + a_{n-k} (k = 2, \ \cdots, n)$$

Il est commode de faire le tableau suivant (le schéma de Hörner)

	a_n	a_{n-1}	$\cdots$	a_1	a_0
c	$b_{n-1} = a_n$	$b_{n-2} = c b_{n-1} + a_{n-1}$	$\cdots$	$b_0 = c b_1 + a_1$	$f(c) = c b_0 + a_0$

En particulier, pour un nombre $n = \sum_{i=0}^{r} c_i m^i$ on considère le polynôme

$f(x) = g_n(x) = \sum_{i=0}^{r} c_i x^i$, et $x = m$ on obtient

	c_r	c_{r-1}	$\cdots$	c_1	c_0
m	$b_{r-1} = c_r$	$b_{r-2} = mb_{r-1} + c_{r-1}$	$\cdots$	$b_0 = mb_1 + c_1$	$g_n(m) = mb_0 + c_0$

Ces méthodes d'addition, de multiplication, de division avec reste, de passage d'une forme d'écriture à une autre donnent des exemples d'algorithmes. On va appeller *algorithme* une procédure de calcul décrite pas par pas. On appelle *algorithme polynômial* de calcul sur des nombres naturels n_1, n_2, ..., n_r, décrits à l'aide de k_1, k_2, ..., k_r bit respectivement, un algorithme avec le temps d'éxécution inférieur où égal à $\mathcal{O}(k_1^{d_1} k_2^{d_2} \cdot ... \cdot k_r^{d_r})$ (pour des constantes d_1, d_2, ..., $d_r \in \mathbb{N}$).

Dans ce qui suit on va donner d'autres exemples des algorithmes polynômiaux : exponentiation modulo un nombre naturel fixé, algorithme d'Euclide.

Cela ne signifie en rien que la recherche des facteurs premiers d'un nombre entier soit un travail facile en général. La "preuve" en est que la cryptographie moderne réside essentiellement sur la difficulté technique de factorisation de grands nombres entiers en produit de nombres premiers.

Problème de Gauss : *Existe-t-il un algorithme pour factorisation de tout nombre donné n qui marche aussi rapide que son "temps d'execution" soit borné par un polynôme du nombre de chiffres décimales de n ?*

La plupart des mathematicians pensent que la réponse est négative, mais personne ne l'a encore prouvé rigoureusement. S'il existait un tel algorithme, alors les cryptosystèmes qu'on utilise pour les transactions interbancaires peuvent être facilement "cassés".

Difficulté comparative de la multiplication et de la factorisation de nombres entiers.

Considérons le développement

$$(10^{71} - 1)/9 = 241573142393627673576957439049 \times \\ \times 459948113478868463102217288952230343018 39.$$

Avec une certaine patience on peut multiplier les deux facteurs pendant quelques heures :

```
> 241573142393627673576957439049*459948113478868463102217288952230343018
> 839;
```

```
111111111111111111111111111111111111111111111111111111111111111111111\
111111
```

Cependant, pour trouver une telle factorisation par la méthode standard de la division successive on aurait besoin de 10^{10} ans de travail des ordinateurs qui font une division en 10^{-9} seconds. En effet, on a réussi à trouver cette factorisation à l'aide du superordinateur CRAY-I en utiisant certains algorithmes très fins qui rendent ce travail abordable. L'estimation des meilleurs algorithmes modernes de factorisation d'un nombre $n \in \mathbb{N}$ est $(\exp(C(\log n)^{1/3}(\log\log n)^{2/3})$.

Difficulté de la vérifications de primalité.

D'autre part, il existe des méthodes assez rapides pour vérification de primalité des grand nombres. Par exemple, un mathematicien canadien H.Willams a démontré en 1988 que le nombre $(10^{1031} - 1)/9$

est premier. Actuellement on peut vérfier sur les ordinateurs la *primalité* d'un nombre naturel avec 100 digits (c'est à dire, la propriété d'être premier) en quelques minutes.

Dans un travail récent de Manindra Agrawal, Neeraj Kayal and Nitin Saxena un algorithme polynômial a été trouvé pour *vérifier* la primalité d'un nombre naturel (*sans trouver* un seul facteur). L'algorithme utilise une version polynômial du "petit théorème de Fermat", et son "temps d'execution" est borné par $\mathcal{O}(\log n)^{12}$ du nombre de chiffres décimales de n (voir le manuscript "Primes is in P" de 2002).

Un défi ("challenge") à $10,000

Dès mois de février 2002, si vous arrivez à factoriser le nombre suivant de 174-chiffres décimales, connu sous le nôm "RSA-576", alors la companie RSA vous payera DIX MILLE DOLLARS !

188198812920607963838697239461650439807163563379417382700 7
633564229888597152346654853190606065047430453173880113033 9
671619969232120573403187955065699622130516875930765025705 9

Ce nombre est appelé RSA-576, car il possède 576 chiffres binaires. Voir [Stein], Chap. 1, et

http ://www.rsasecurity.com/rsalabs/challenges/factoring/index.html

pour les details (il y a même un défi à $200,000).

1.3 Application à la multiplication rapide.

Il est clair, que les opérations algébriques (l'addition, la multiplication, l'exponentiation) dans les anneaux sont très importantes ; c'est pourquoi on va considérer des méthodes commodes pour effectuer ces opérations.

Soit m un entier strictement positif. Alors on peut voir l'écriture en base m d'un entier positif

$$n = (c_{k-1} \cdots c_1 c_0)_m$$

(i.e.

$$n = \sum_{i=0}^{k-1} c_i m^i \text{ avec } 0 \leq c_i \leq m-1)$$

comme un analogue d'un polynôme $g_n(x) = \sum_{i=0}^{r} c_i x^i$ parce que $n = g(m)$. Pour multiplier deux nombres n et $n' = \sum_{i=0}^{r} c'_i x^i$ on peut utiliser une *multiplication rapide* des polynômes : $g_{n'}(x) = \sum_{i=0}^{r} c'_i x^i$, $n' = g_{n'}(m)$, alors

$$nn' = g_n(m) g_{n'}(m) = (g_n g_{n'})(m).$$

Un exemple modèle pour la multiplication rapide des nombres et des polynômes est donné par la règle :

$$(ax+b)(cx+d) = ac(x^2+x) + (b-a)(c-d)x + bd(x+1) \tag{1.2}$$

donc la multiplication des polynômes de degré ≤ 1 nécessite seulement 3 multiplications essentiels au lieu de 4 multiplications par la méthode traditionnelle. On utilise cette règle avec $x = 2^l$.

Rapellons que l'algorithme traditionnel pour la multiplication de deux nombres de $\leq k$ chiffres binaires ($m = 2$) nécessite $\leq k^2$ opérations élémentaires (de type $1_2 + 1_2 = 10_2$).

La règle (1.2) amène à un algorithme rapide de multiplication dont le temps d'execution est majoré par $\mathcal{O}(k^{\log_2 3})$.

1.4 pgcd, ppcm

DÉFINITION 1.4.1 *Soit I un ensemble et $(a_i)_{i\in I}$ une famille d'entiers.*

(i) On dit que $d \in \mathbb{N}$ est un pgcd de la famille $(a_i)_{i\in I}$ si

$$\forall (i \in I, d|a_i) \text{ et } \forall r \in \mathbb{Z}, \forall (i \in I, r|a_i) \Rightarrow r|d$$

(ii) On dit que $m \in \mathbb{N}$ est un ppcm de la famille $(a_i)_{i\in I}$ si

$$\forall (i \in I, a_i|m) \text{ et } \forall r \in \mathbb{Z}, \forall (i \in I, a_i|r) \Rightarrow m|r$$

NOTATIONS. $r = \text{pgcd}((a_i)_{i\in I})$, $m = \text{ppcm}((a_i)_{i\in I})$.

REMARQUE.

Si $I = \emptyset$, alors le pgcd vaut 0 et ppcm vaut 1. Si $I = \{0\}$ et $a_0 > 0$, alors le pgcd et ppcm coincident avec a_0.

Algorithme d'Euclide pour le calcul de pgcd

Pour des entiers a, b on écrit $a|b$ si a divise b, c'est à dire$b = ad$ pour un entier d. Si p est premier et p^α le plus grande puissance de p divisant n on écrit $p^\alpha \| n$ et $\alpha = ord_p n$. Le théorème de factorisation peut être facilement déduit de son cas particulier : si un nombre premier p divise ab alors soit $p|a$ soit $p|b$. Cette propriété découle de l'algorithme d'Euclide.

Si l'on connait les factorisations de a et b en produit de nombres premiers on voit directement l'existence et la forme explicite du plus grand commun diviseur (notation : $\text{pgcd}(a, b)$) et du plus petit commun multiple (notation $\text{ppcm}(a, b)$). Notamment, posons $m_p = \min(ord_p(a), ord_p(b))$, $g_p = \max(ord_p(a), ord_p(b))$. Alors

$$\text{pgcd}(a, b) = \prod_p p^{m_p}, \quad \text{ppcm}(a, b) = \prod_p p^{g_p}.$$

Un fait surprenant est qu'on peut calculer facilement le pgcd, par exemple $\text{pgcd}(2261, 1275)$, sans utiliser la factorisation. Plus précisemment :

$$2261 = 1 \cdot 1275 + 986.$$

On remarque que le nombre d divise tous les deux 2261 et 1275, alors d divise automaticment leur différence 986.

De même façon, si un nombre divise les deux 1275 et 986, alors il divise aussi leur somme 2261. Donc on progrèsse :

$$\text{pgcd}(2261, 1275) = \text{pgcd}(1275, 986).$$

Essayons encore :

$$1275 = 1 \cdot 986 + 289,$$

donc $\text{pgcd}(1275, 986) = \text{pgcd}(986, 289)$:

$$986 = 3 \cdot 289 + 119$$
$$289 = 2 \cdot 119 + 51$$
$$119 = 2 \cdot 51 + 17.$$

Ceci dit, $\text{pgcd}(2261, 1275) = \cdots = \text{pgcd}(51, 17)$, i.e. 17 car $17 \mid 51$, et

$$\text{pgcd}(2261, 1275) = 17.$$

Cette méthode est très efficace et elle donne l'algorithme classique suivant :

Algorithme d'Euclide :

On fix $a, b \in \mathbb{N}$ avec $a > b$. En utilisant "division avec reste" (division euclidienne), on écrit

$$a = bq + r, \text{avec } 0 \leq r < b. \tag{1.3}$$

Alors, comme ci-dessus,

$$\text{pgcd}(a, b) = \text{pgcd}(b, r).$$

On pose $a_1 = b$, $b_1 = r$, et on répète jusqu'a $r = 0$. On calcule assez rapidement $\text{pgcd}(a, b)$. L'algorithme d'Euclide se compose donc du calcul d'une suite

$$d_0, \quad d_1, \quad d_2, \ldots$$

où $d_0 = a, \quad d_1 = b$ et d_{i+1} est le residu de d_{i-1} modulo d_i :

$$d_{i+1} = d_{i-1} - td_i.$$

On s'arrête lorsque $d_k = 0$; alors $d_{k-1} = \text{pgcd}(a, b)$. On peut montrer (en exercice) que le nombre des divisions est borné par $5 \log_{10} \max(a, b)$ (*le théorème de Lamé*).

THÉORÈME 1.4.2 *Soit $a, b \in \mathbb{N}$ des entiers positifs. Alors il existe* $\text{pgcd}(a, b)$.

PREUVE. On observe simplement que $d = d_{k-1} = \text{pgcd}(a, b)$ satisfait les conditions de définition 1.4.1.

EXEMPLE. On pose $a = 15$ et $b = 6$.

$$\begin{aligned} 15 &= 6 \cdot 2 + 3 \qquad \text{pgcd}(15, 6) = \text{pgcd}(6, 3) \\ 6 &= 3 \cdot 2 + 0 \qquad \text{pgcd}(6, 3) = \text{pgcd}(3, 0) = 3 \end{aligned}$$

EXEMPLE. Soit $a = 150$ et $b = 60$.

$$\begin{aligned} 150 &= 60 \cdot 2 + 30 \qquad \text{pgcd}(150, 60) = \text{pgcd}(60, 30) \\ 60 &= 30 \cdot 2 + 0 \qquad \text{pgcd}(60, 30) = \text{pgcd}(30, 0) = 30 \end{aligned}$$

Avec l'algorithme d'Euclide on va prouver maintenant que si un nombre premier divise le produit de deux nombres entiers, alors il divise l'un d'eux. Ce résultat est la clé pour prouver l'unicité de factorisation.

THÉORÈME 1.4.3 (LEMME D'EUCLIDE) *Soit p un nombre premier et $a, b \in \mathbb{N}$ des entiers positifs. Si $p \mid ab$ alors $p \mid a$ ou $p \mid b$.*

PREUVE. Si $p \mid a$, c'est fait. Si $p \nmid a$ alors $\text{pgcd}(p, a) = 1$, car seulement 1 et p divisent p. A partir de l'algorithme d'Euclide, on voit $\text{pgcd}(pb, ab) = b$. A chaque étape on multiplie l'equation par b. Comme $p \mid pb$ et, par l'hypothèse, $p \mid ab$, on obtient que $p \mid \text{pgcd}(pb, ab) = b$.

COROLLAIRE 1.4.4 *Soit p un nombre premier, $s \in N$, et $a_1, \cdots, a_s \in \mathbb{N}$ des entiers positifs. Si $p \mid a_1 \cdot \ldots \cdot a_r$ alors p divise l'un des a_i : $\exists p \mid a_i$.*

Unicité de décomposition

d'un entier positif n en produit de nombres premiers est directement impliquée par le Lemme d'Euclide 1.4.3 (et son corollaire 1.4.4) : soient $r, s \in \mathbb{N}$, $p_1, \cdots, p_r$ et $q_1, \cdots, q_s$ des nombres premiers tels que

$$n = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s$$

alors $r = s$ et $p_1, \cdots, p_r$ coïncident $q_1, \cdots, q_s$ à une permutation près.

En effet, on peut supposer $r \geq s$. On procède par récurrence sur r. Si r=0, alors n=1, $s = 0$, et le résultat annoncé est vrai. Supposons le résultat montré pour $r - 1$ avec $r \geq 1$. On a

$$p_1 | q_1 \cdot \ldots \cdot q_s.$$

Donc p_1 divise l'un des q_i.

Quitte à échanger les q_i, on peut supposer que $p_1 | q_1$. Comme le nombre q_1 est premier, on obtient $p_1 = q = 1$, d'où

$$p_2 \cdot \ldots \cdot p_r = q_2 \cdot \ldots \cdot q_s$$

(après la simplification), et il reste à appliquer l'hypothèse de récurrence au produit $p_2 \cdot \ldots \cdot p_r$ de $r - 1$ nombres premiers.

EXERCICE 1.4.5 *Montrer que si* $a_1, a_2 > 0$,

$$\mathrm{pgcd}(a_1, a_2) \cdot \mathrm{ppcm}(a_1, a_2) = a_1 \cdot a_2$$

EXERCICE 1.4.6 *Algorithmes pour calculer le pgcd d'une famille finie* $\{a_1, \cdots, a_r\}$. *Montrer par récurrence que*

$$\mathrm{pgcd}(a_1, \cdots, a_r) = \mathrm{pgcd}(\mathrm{pgcd}(a_1, \cdots, a_{r-1}), a_r),$$

et que

$$\mathrm{ppcm}(a_1, \cdots, a_r) = \mathrm{ppcm}(\mathrm{ppcm}(a_1, \cdots, a_{r-1}), a_r),$$

Programme pour trouver le pgcd (en Maple)

```
> restart;
> a:=691;
> b:=-1000;
> i:=0;
> if a<0 then a:=-a;
> else fi;
> if b<0 then b:=-b;
> else fi;
> while(b<>0) do
> i:=i+1;
> r:=irem( a,b );
> a:=b;
> b:=r;
> od;
> print(i, a);
```

$$a := 691$$
$$b := -1000$$
$$i := 0$$

$b := 1000$
$i := 1$
$r := 691$
$a := 1000$
$b := 691$
$i := 2$
$r := 309$
$a := 691$
$b := 309$
$i := 3$
$r := 73$
$a := 309$
$b := 73$
$i := 4$
$r := 17$
$a := 73$
$b := 17$
$i := 5$
$r := 5$
$a := 17$
$b := 5$
$i := 6$
$r := 2$
$a := 5$
$b := 2$
$i := 7$
$r := 1$
$a := 2$
$b := 1$
$i := 8$
$r := 0$
$a := 1$
$b := 0$
8, 1

Procédure pour trouver le pgcd (en Maple-7)

```
> pgcd:=proc(a::integer,b::integer)
> local r,d0,d1,i;
> i:=0;
> if a<0 then a:=-a;
> else fi;
> if b<0 then b:=-b;
> else fi;
> r:=b;
> d0:=a; d1:=b;
> r:=b;
> while(d1<>0) do
> i:=i+1;
> r:=irem( d0,d1 );
> d0:=d1;
> d1:= r;
> od;
> return d0;
> end proc;
```

$$
\begin{aligned}
&\mathit{pgcd} := \mathbf{proc}(a::\mathit{integer},\ b::\mathit{integer})\\
&\mathbf{local}\ r,\ \mathit{d0},\ \mathit{d1},\ i;\\
&\quad i := 0\,;\\
&\quad \mathbf{if}\ a < 0\ \mathbf{then}\ a := -a\ \mathbf{else\ end\ if};\\
&\quad \mathbf{if}\ b < 0\ \mathbf{then}\ b := -b\ \mathbf{else\ end\ if};\\
&\quad r := b\,;\\
&\quad \mathit{d0} := a\,;\\
&\quad \mathit{d1} := b\,;\\
&\quad r := b\,;\\
&\quad \mathbf{while}\ \mathit{d1} \neq 0\ \mathbf{do}\ i := i+1\,;\ r := \mathrm{irem}(\mathit{d0},\ \mathit{d1})\,;\ \mathit{d0} := \mathit{d1}\,;\ \mathit{d1} := r\ \ \mathbf{end\ do}\,;\\
&\quad \mathbf{return}\ \mathit{d0}\\
&\mathbf{end\ proc}
\end{aligned}
$$

```
> pgcd(12,14);
```

$$2$$

```
> pgcd(91,65);
```

$$13$$

```
> pgcd(2261,1275);
```

$$17$$

1.5 Congruences

DÉFINITION 1.5.1 *Si a, b sont deux entiers relatifs, on dit que a est congru à b modulo m et on note*

$$a \equiv b \bmod m$$

si et seulement si m divise $a - b$.

PROPOSITION 1.5.2 *Si a, b, c, d, m et n sont des entiers relatifs,*

(i) $a \equiv a \bmod m$,
(ii) si $a \equiv b \bmod m$, *alors* $b \equiv a \bmod m$,
(iii) si $a \equiv b \bmod m$ *et* $b \equiv c \bmod m$, *alors* $a \equiv c \bmod m$,
(iv) si m est non nul et si b est le reste de la division euclidienne de a par m, alors on a $a \equiv b \bmod m$,

v) si $a \equiv b \bmod m$ *et si* $n|m$*, alors on a* $a \equiv b \bmod n$*,*
(vi) si $a \equiv b \bmod m$ *et* $c \equiv d \bmod m$*, alors* $a + c \equiv b + d \bmod m$*,*
(vii) si $a \equiv b \bmod m$ *et* $c \equiv d \bmod m$*, alors* $ac \equiv bd \bmod m$*,*
(viii) si $a \equiv b \bmod m$ *et si* n *est un entier positif, alors* $a^n \equiv b^n \bmod m$*.*

PREUVE. C 'est un exercice facile. Montrons (vii) à titre d'exemple : si $a \equiv b \bmod m$, et $c \equiv d \bmod m$, alors il existe des entiers relatifs q_1 et q_2 tels que

$$a - b = mq_1 \text{ et } c - d = mq_2;$$

par conséquant,

$$ac - bd = (a - b)c + b(c - d) = m(q_1 + q_2);$$

d'où l'assertion.

EXEMPLE 1.5.3
Si a *est entier positif ou nul et* $a_r a_{r-1} \cdots a_0$ *son écriture en base 10 (i.e.* $a = \sum_{i=0}^{r} a_i 10^i$*), alors*
(i) $a \equiv a_0 (\mathrm{mod} 10)$*,*
(ii) $a \equiv \sum_{i=0}^{r} a_i (\mathrm{mod} 9)$
(iii) $a \equiv \sum_{i=0}^{r} (-1)^i a_i (\mathrm{mod} 11)$

Règles de divisibilité

PROPOSITION 1.5.4 *Un nombre* $n \in \mathbb{Z}$ *est divisible par* 3 *si et seulement si la somme des chiffres décimales de* n *est divisible par* 3*.*

PREUVE. On écrit

$$n = a + 10b + 100c + \cdots .$$

Comme 10≡1 (mod 3),

$$n = a + 10b + 100c + \cdots \equiv a + b + c + \cdots \pmod 3,$$

d'où la proposition.

De même façon, on trouve les règles de divisibilité par 5, 2, 4, 9 et 11 (voir exemple 1.5.3).

EXERCICE 1.5.5 *Proposer une règle de divisibilité par* 7*, utilsant les faits* $10 \equiv 3 (\mathrm{mod} 7)$*,* $100 \equiv 2 (\mathrm{mod}$ $7)$*,* $1000 \equiv -1 (\mathrm{mod} 7)$*.*

EXERCICES

1.1 Proposer une règle de divisibilité par 13, en utilisant $1001 = 7 \cdot 11 \cdot 13$.

1.2 Calculer de tête le dernier chiffre de l'écriture en base 10 des nombres suivants : 2309786^{34657}, $8786652^{35444619}$ et $654565198^{3548217}$.

1.3 alculer de tête le reste de la division par 9 des nombres suivants : $8^{68498353}$, 54648381^{54648} et 354872846^{21353}.pey12

1.4 Existe-t-il des nombres entiers x, y tels que $x^2 + y^2 = 2003$?

1.5 Existe-t-il des nombres entiers x, y tels que $x^2 + 5y^2 = 2003$?

1.6 Soit b un entier strictement positif, énoncer et démontrer l'analogue de l'exemple 1.5.3 pour l'écriture en base b d'un entier positif a (i.e. $a = \sum_{i=0}^{r} a_i b^i$ avec $0 \leq a_i \leq b - 1$).

1.7 Trouver tous entiers n tels que la fonction f_n (definite par l'égalité(1.1)) ne s'annule pas.

1.8 Déssiner la fonction f_{15}.

1.9 La fonction f_n est-elle croissante (decroissante) ?

1.10 Justifier la procédure suivante pour calculer les l derniers chiffres en base d d'un nombre entier positif n :

```
> restart;
> Chiffres:= proc(  d::nonnegint,l::nonnegint,n::nonnegint )
> local i,m, v;
> v:=vector(l);
> m:=n;
> for i from 0 to l-1 do
> v[l-i]:=modp(m,d);m:=floor(m/d); od;
> return v;
> end proc;
```

$$\begin{array}{l} \mathit{Chiffres} := \mathbf{proc}(d :: \mathit{nonnegint},\ l :: \mathit{nonnegint},\ n :: \mathit{nonnegint}) \\ \quad \mathbf{local}\, i,\ m,\ v; \\ \qquad v := \mathrm{vector}(l)\,; \\ \qquad m := n\,; \\ \qquad \mathbf{for}\, i\, \mathbf{from}\, 0\, \mathbf{to}\, l-1\, \mathbf{do}\, v_{l-i} := \mathrm{modp}(m,\ d)\,;\ m := \mathrm{floor}(m/d)\, \mathbf{end\ do}\,; \\ \qquad \mathbf{return}\ v \\ \quad \mathbf{end\ proc} \end{array}$$

```
> evalm(Chiffres(2,12, 127));
```

$$[0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1]$$

```
> evalm(Chiffres(7,5,700));
```

$$[0,\ 2,\ 0,\ 2,\ 0]$$

vérification :2*7+2*7^3=700 ?

```
> 2*7+2*7^3=700;
```

$$700 = 700$$

1.11 Trouver tous entiers x, y, z tels que

$$x^3 + 2y^3 + 4z^3 = 0.$$

1.12 Combien de zéros se trouvent à la fin de 20! ?

1.13 Montrer que si $2^p - 1$ est premier alors $2^{p-1}(2^p - 1)$ est *parfait*, c'est à dire, il est égal à la somme de ses diviseurs propres (e.g. $6 = 1+2+3$, $28 = 1+2+4+7+14$, $496 = 1+2+4+8+16+31+62+124+248$) (Euler a démontré que tous les nombres pairs parfaits sont de ce type).

1.14 Trouver une formule explicite pour les nombres de Fibonacci $a = u_k$, $b = u_{k-1}$ où $u_0 = u_1 = 1$ et $u_{i+1} = u_i + u_{i-1}$:

$$u_i = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^{i+1} - \left(\frac{1-\sqrt{5}}{2} \right)^{i+1} \right).$$

1.15 On definit le nombre d'or comme la solution positive de la proportion d'or

$$\frac{1}{x} = \frac{x}{1-x}$$

("le quotient de l'unité par une partie est égale au quotient de cette partie par la partie complémentaire"), c'est à dire $x = \frac{\sqrt{5}-1}{2}$. Montrer que

$$\frac{u_i}{u_{i+1}} \to \frac{2}{1+\sqrt{5}} = \frac{\sqrt{5}-1}{2}.$$

1.16 Soient a, k, l des nombres entiers positifs. Trouver

$$\mathrm{pgcd}(a^k - 1, a^l - 1).$$

Cours N°2. Jeudi le 9 octobre 2003

2 Entiers modulo n

2.1 Relations d'équivalence et ensembles quotients

La congruence est une relation d'équivalence. Rappellons ce dont il s'agit.

DÉFINITION 2.1.1 *Une* relation binaire $\mathcal{R}$ *sur un ensemble* E *est une partie*

$$E_{\mathcal{R}} \subset E \times E = \{(a,b) \mid a,b \in E\}$$

on écrit $a \overset{\mathcal{R}}{\sim} b$ *si et seulement si* $(a,b) \in E_{\mathcal{R}}$

DÉFINITION 2.1.2 *Une relation binaire* $\mathcal{R}$ *sur un ensemble* E *est une* relation d'équivalence *si et seulement si elle vérifie les trois conditions suivantes :*

- Réflexive. $\forall a \in E$, $a \overset{\mathcal{R}}{\sim} a$.
- Symétrique. *Si* a *et* b *appartiennent à* E *et si* $a \overset{\mathcal{R}}{\sim} b$, *alors* $b \overset{\mathcal{R}}{\sim} a$
- Transitive. *Si* a, b *et* c *appartiennent à* E *et si* $a \overset{\mathcal{R}}{\sim} b$ *et* $b \overset{\mathcal{R}}{\sim} c$, *alors* $a \overset{\mathcal{R}}{\sim} c$

Pour tout x de E on appelle classe d'équivalence de x modulo $\mathcal{R}$, notée $\overline{x}$, la partie

$$\{y \in E \mid y \overset{\mathcal{R}}{\sim} x\}$$

de E. On dit également que x est un représentant de la clase d'équivalence $\overline{x}$.

L'ensemble des classes d'équivalence modulo $\mathcal{R}$ est appelé ensemble-quotient de E par $\mathcal{R}$. On le note $E/\mathcal{R}$.

PROPOSITION 2.1.3 *L'exsemble quotient* $E/\mathcal{R}$ *forme une partition de* E *autrement dit aucune classe d'équivalence n'est vide et deux classes d'équivalence sont soit disjointes soit identiques.*

DÉFINITION 2.1.4 *L'application*

$$E \to E/\mathcal{R}, x \mapsto \overline{x}$$

est surjective, on l'appele la projection canonique.

2.2 Arithmétique modulo n

PROPOSITION 2.2.1 *Pour tout entier* n *la relation de congruence* $x \equiv y \bmod n$ *est une relation d'équivalence sur* $\mathbb{Z}$. *On note* $\mathbb{Z}/n\mathbb{Z}$ *l'ensemble quotient associé.*

PREUVE. Il suffit d'utiliser les propriétés (i), (ii) et (iii) de Proposition 1.5.2. La propriété (iv) montre que

$$\mathbb{Z} = \overline{0} \cup \overline{1} \cup \cdots \cup \overline{n-1} = n\mathbb{Z} \cup (1+n\mathbb{Z}) \cup \cdots \cup (n-1+n\mathbb{Z})$$

On suppose $a, a', b, b' \in \mathbb{Z}$ et

$$a \equiv a' \pmod{n}, \qquad b \equiv b' \pmod{n}.$$

Alors

$$a + b \equiv a' + b' \pmod{n} \tag{2.1}$$

$$a \cdot b \equiv a' \cdot b' \pmod{n} \tag{2.2}$$

Ceci permet de definir une addition $+$ et une multiplication $\times$ (ou $\cdot$) sur $\mathbb{Z}/n\mathbb{Z}$ par les formules

$$\overline{a} + \overline{b} = \overline{a+b} \text{ et } \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Ceci implique que si $m > 0$ la puissance m-ème d'un élément a de $\mathbb{Z}/n\mathbb{Z}$ est donné par

$$\overline{a}^m = \overline{a^m}.$$

De point de vue pratique, ces calculs peuvent être implémentés de la façon suivante : pour l'addition

ALGORITHME 2.2.2

Entrée *:*

– *Entier n de congruence.*

– *Entiers a et b (entre 0 et $n-1$).*

Sortie :

– *Représentant de $a+b$ (entre 0 et $n-1$).*

Algorithme :

– *Calculer $c = a + b$.*

– *Calculer le reste r de la division de c par n.*

Un algorithme analogue peut être écrit pour la *multiplication*.

Pour *l'exponentiation*, il convient de minimiser le nombre de multiplications effectuées. L'idée pour cela est de considerer l'écriture en base 2 de la puissance cherchée :

$$m = \sum_{i=0}^{r} m_i 2^i \text{ avec } m_i = 0 \text{ ou } 1.$$

On a la relation

$$\overline{a}^m = \prod_{\substack{0 \le i \le r \\ m_i = 1}} \overline{a}^{2^i}.$$

La formule

$$m = m_r 2^r + \cdots + m_0 = 2(2(\cdots 2(2m_r + m_{r-1}) + \dots) + m_1) + m_0$$

montre que dans cet exemple

$$\begin{aligned} \overline{a}^m &= \overline{a}^{2(2(\cdots 2(2m_r + m_{r-1}) + \dots) + m_1) + m_0} \\ &= (\cdots((\overline{a}^{m_r})^2 \overline{a}^{m_{r-1}})^2 \cdots)^2 \overline{a}^{m_0} \end{aligned}$$

ALGORITHME 2.2.3

Entrée *:*

– *Entier n de congruence.*

– *Puissance m.*

–*Element a de $\mathbb{Z}/n\mathbb{Z}$*

Sortie :

– *Valeur de a^m dans $\mathbb{Z}/n\mathbb{Z}$.*

Algorithme :

1. $x := a$, $y = m$;

2. $z := 1$;

3. Tant que y n'est pas nul

3.1 si y est impaire, $z := z * x \bmod n$

3.2 $x := x * x \bmod n$

3.3 $m := m/2$

4. renvoyer z

2.3 Une procédure pour calcul de $a^m \bmod n$ en Maple

On peut simplement utiliser

```
> a &^ m mod n;
```

Sinon, on écrit une procédure :

```
> Puismod:=
> proc(a::nonnegint, m::nonnegint, n::nonnegint)
> local x, y, z, mi;
> x:=a;
> y:=m;
> z:=1;
> while (y<>0) do
> mi:=y mod 2;
> if (mi=1) then z := z*x mod n;
> else fi;
> x:=x*x mod n;
> y:=floor(y/2);
> printf("mi=%d, x=%d, y=%d, z=%d\n",mi,x,y,z)
> od;
> return z;
> end proc;
```

$$
\begin{array}{l}
Puismod := \mathbf{proc}(a::nonnegint,\ m::nonnegint,\ n::nonnegint) \\
\mathbf{local}\ x,\ y,\ z,\ mi; \\
\quad x := a\,; \\
\quad y := m\,; \\
\quad z := 1\,; \\
\quad \mathbf{while}\ y \neq 0\ \mathbf{do} \\
\qquad mi := y \bmod 2\,; \\
\qquad \mathbf{if}\ mi = 1\ \mathbf{then}\ z := z * x \bmod n\ \mathbf{else\ end\ if}; \\
\qquad x := x^2 \bmod n\,; \\
\qquad y := \mathrm{floor}(1/2 * y)\,; \\
\qquad \mathrm{printf}(\text{“mi=\%d, x=\%d, y=\%d,\ z=\%d\textbackslash n”},\ mi,\ x,\ y,\ z) \\
\quad \mathbf{end\ do}; \\
\quad \mathbf{return}\ z \\
\mathbf{end\ proc}
\end{array}
$$

```
> Puismod(2,11,100);
```

```
mi=1, x=4, y=5, z=2

mi=1, x=16, y=2, z=8

mi=0, x=56, y=1, z=8

mi=1, x=36, y=0, z=48
```

48

vérification :

```
> 2^11;
```

2048

Simplification dans $\mathbb{Z}/n\mathbb{Z}$

PROPOSITION 2.3.1 *Si* $\text{pgcd}(c,n)=1$ *et*

$$ac \equiv bc \pmod{n}$$

alors $a \equiv b \pmod{n}$.

PREUVE. Par définition

$$n \mid ac - bc = (a-b)c.$$

Comme $\text{pgcd}(n,c)=1$, on a $n \mid a-b$, donc

$$a \equiv b \pmod{n},$$

d'où la proposition.

COROLLAIRE 2.3.2 *Si* $\text{pgcd}(c,n)=1$ *alors l'application* $x \mapsto cx$ *de* $\mathbb{Z}/n\mathbb{Z}$ *dans* $\mathbb{Z}/n\mathbb{Z}$ *est bijective, en particulier, pour tout* b *dans* $\mathbb{Z}/n\mathbb{Z}$ *il existe un seul* x *dans* $\mathbb{Z}/n\mathbb{Z}$ *tel que*

$$ax \equiv b \pmod{n}.$$

EXERCICES

2.1. *Justifier une version de l'algorithme d'Euclide donnée par la division avec reste de plus petite valeur absolue :*

$$\begin{aligned}
&x_0 = a_0 x_1 + \varepsilon_1 x_2,\\
&x_1 = a_1 x_2 + \varepsilon_2 x_3, \ \ldots, \quad 0 \le x_k < x_{k-1}/2, \quad \varepsilon_i = \pm,\\
&\cdots\cdots\cdots\cdots\\
&x_{n-1} = a_{n-1} x_n.
\end{aligned}$$

2.2. *Posons* $D_0 = 0$, $D_1 = 1$, $\ldots$, $D_n = 2D_{n-1} + D_{n-2}$.
(la suite des nombres de Dupré). Démontrer : Théorème (Athanase Dupré, 1846) Soient u, $v > 0$ *des nombres naturels tels que l'algorithme d'Euclide marche pour* n *divisions (avec reste de plus petite valeur absolute), et* u *est minimal avec cette propriété. Alors*

$$u = D_n + D_{n-1}, \quad v = D_n,$$

2.3. *En déduire : Pour* (u, v), $u > v > 0$, *l'algorithe d'Euclide marche pour au plus*

$$1,14 \log u - 0,79 + 0,41 u^{-1}$$

divisions avec reste de plus petite valeur absolue.

Solution : voir [Knuth, p. 605]. On utilise ci–dessus la formule

$$D_n = \frac{1}{2\sqrt{2}} \left((1+\sqrt{2})^n - (1-\sqrt{2})^n \right).$$

3 Rappels sur la notion de groupe, exemples

3.1 Structure de groupe

Définition 3.1.1 *Un groupe est un ensemble G muni d'une loi interne*

$$G \times G \to G, \quad (x, y) \mapsto xy = x \cdot y$$

qui est associative

Gr1 $\forall x, y, z \in G, x(yz) = (xy)z$,

admet un element neutre e :

Gr2 $\forall x \in G, xe = ex = x$,

et tout élément x du groupe G admet un inverse (ou symétrique) y :

Gr3 $\forall x \in G, \exists y \in G, xy = yx = e$,

cet élément est alors unique, on le note x^{-1}.

En outre le groupe G est dit commitatif ou abélien s'il vérifie également la condition suivante :

Comm. $\forall x, y \in G, xy = yx$.

Remarque 3.1.2 *On prend souvent une notation additive pour la loi d'un groupe abélien, la loi s'écrira alors $(x, y) \mapsto x + y$, l'élément neutre sera noté 0 et le symétrique (où opposé) d'un élément x sera noté $-x$.*

Exemple 3.1.3

L'ensemble $\mathbb{Z}$ muni de l'addition est un groupe commutatif. Il est de même pour $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ muni de l'addition. L'addition muni également $\mathbb{Z}/n\mathbb{Z}$ d'une structure de groupe abélien.

Définition 3.1.4 *Un groupe G est dit* monogène*, s'il existe un élément g de G tel que $\{g\}$ engendre G, i.e. pour tout $h \in G$ il existe un entier positif n tel que soit $h = g^n$ soit $h = g^{-n} = (g^{-1})^n$. On dit alors que g est un* générateur *de G. Un groupe monogène fini est dit* cyclique*.*

En particulier, le groupe additif $\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre n et de générateur $\overline{1}$:

$$\overline{1} + \overline{1} = \overline{2}, \overline{1} + \overline{1} + \overline{1} = \overline{3}, \cdots$$

Le groupe additif $\mathbb{Z}$ est monogène de générateur 1 (ou de générateur -1).

Exercice 3.1.5 *Trouver tous les générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$. Montrer qu'une classe $\overline{a} = a \bmod n$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$ si et seulement si* $\operatorname{pgcd}(a, n) = 1$.

Exemple 3.1.6

Si X est un ensemble, l'ensemble des bijections de X dans X, aussi appelées permutations *de X, forment un groupe pour la loi de composition que l'on note $\mathfrak{S}_X$. On note $\mathfrak{S}_n$ pour le* groupe des permutatons *de $\{1, \cdots, n\}$. Si $n \geq 3$, alors ce groupe n'est pas abélien.*

Définition 3.1.7

(a) Soient G et H deux groupes. Une application $\phi : G \to H$ est un morphisme *de groupes si elle vérifie la condition*

Mor $\forall x, y \in G, \phi(xy) = \phi(x)\phi(y)$.

(b) Un isomorphisme *de groupes est un morphisme de groupes qui est bijectif. Son inverse est alors un isomorphism de groupes.*

(c) Un automorphisme *d'un groupe G est un isomorphisme de G dans G. Son inverse est alors un automorphisme de G.*

Exercice 3.1.8 *Trouver tous les morphismes du groupe $\mathbb{Z}/10\mathbb{Z}$ dans $\mathbb{Z}/12\mathbb{Z}$.*

Exercice 3.1.9 *Trouver tous les automorphismes des groupes $\mathbb{Z}/10\mathbb{Z}$ et $\mathbb{Z}/12\mathbb{Z}$.*

3.2 Exemple : éléments inversibles $\mod n$.

Rapellons que pour un élément $a \bmod n \in \mathbb{Z}/n\mathbb{Z}$ l'application $x \mapsto ax$ de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ est bijective si et seulement si $\text{pgcd}(a, n) = 1$, en particulier, dans ce cas pour tout b dans $\mathbb{Z}/n\mathbb{Z}$ il existe un seul x dans $\mathbb{Z}/n\mathbb{Z}$ tel que

$$ax \equiv b \pmod{n}.$$

(voir Corollaire 2.3.2).

Définition 3.2.1 *On appelle groupe d'éléments inversibles* $\mod n$ *l'ensemble d'éléments* $a \bmod n \in \mathbb{Z}/n\mathbb{Z}$ *tels que* $\text{pgcd}(a, n) = 1$, *et on le note* $(\mathbb{Z}/n\mathbb{Z})^\times$. *L'élément neutre* e *de* $(\mathbb{Z}/n\mathbb{Z})^\times$ *est la classe* $1 \bmod n = 1 + n\mathbb{Z}$, *et l'élément symétrique de* $a \bmod n$ *et la classe* $x \bmod n$, *où* $ax \equiv 1 \pmod{n}$.

Pour trouver un élément x tel que $ax \equiv b \pmod{n}$, il suffit de résoudre l'équation $ax + ny = b$ en entiers x, y, on utilisera une information supplémentaire sur le pgcd donnée par

Proposition 3.2.2 *On suppose* $a, b \in \mathbb{Z}$ *et* $\text{pgcd}(a, b) = d$. *Alors il existe* $x, y \in \mathbb{Z}$ *tels que*

$$ax + by = d.$$

On donne d'abord un exemple concret de calcul de solution d'une équation comme $ax \equiv 1 \pmod{n}$.

Exemple 3.2.3 *Soit* $a = 5$ *et* $b = 7$. *Les étapes de l'algorithme d'Eclide sont :*

$$\begin{aligned} 7 &= 1 \cdot 5 + 2 && \text{donc } 2 = 7 - 5 \\ 5 &= 2 \cdot 2 + 1 && \text{donc } 1 = 5 - 2 \cdot 2 = 3 \cdot 5 - 2 \cdot 7. \end{aligned}$$

A droite, nous avons écrit tout reste comme une combinaison linéaire de a *et de* b. *Finalement, on a écrit* $\text{pgcd}(a, b)$ *comme une combinaison linéaire* a *et* b.

Cet exemple n'été pas compliqué, et on pourrait aborder un exemple plus long.

Exemple 3.2.4 *Soit* $a = 130$ *et* $b = 61$. *Nous avons*

$$\begin{aligned} 130 &= 2 \cdot 61 + 8 && \text{donc } 8 = 130 - 2 \cdot 61 \\ 61 &= 7 \cdot 8 + 5 && \text{donc } 5 = -7 \cdot 130 + 15 \cdot 61 \\ 8 &= 1 \cdot 5 + 3 && \text{donc } 3 = 8 \cdot 130 - 17 \cdot 61 \\ 5 &= 1 \cdot 3 + 2 && \text{donc } 2 = -15 \cdot 130 + 32 \cdot 61 \\ 3 &= 1 \cdot 2 + 1 && \text{donc } 1 = 23 \cdot 130 - 49 \cdot 61. \end{aligned}$$

Alors $x = 130$ *et* $y = -49$.

Remarque 3.2.5 *Il est suffit pour nous de trouver une solution de* $ax + by = d$. *En effet, il existe toujours une infinité de solutions. Si* x, y *est une solution de*

$$ax + by = d,$$

alors pour tous $\alpha \in \mathbb{Z}$,

$$a\left(x + \alpha \cdot \frac{b}{d}\right) + b\left(y - \alpha \cdot \frac{a}{d}\right) = d,$$

est aussi une solution, et toutes les solutions sont de cette forme pour un α.

Identité de Bezout.

L'algorithme d'Euclide se compose du calcul d'une suite

$$d_0, \quad d_1, \quad d_2, \ldots$$

où $d_0 = a, \quad d_1 = b$ et d_{i+1} est le residu de d_{i-1} modulo d_i :

$$d_{i+1} = d_{i-1} - td_i.$$

On s'arrête lorsque $d_k = 0$; alors $d_{k-1} = \text{pgcd}(a, b)$. On peut montrer que le nombre des divisions est borné par $5 \log_{10} \max(a, b)$ (*le théorème de Lamé*).

De l'algorithme d'Euclide provient aussi une représentation

$$\text{pgcd}(a, b) = ua + vb \tag{3.1}$$

où u, v sont des entiers. Pour les construire on calcule successivement les paires (u_i, v_i) tels que $d_i = u_i a + v_i b$. Posons $u_0 = v_1 = 1, u_1 = v_0 = 0$ et pour $i \geq 1$

$$u_{i+1} = u_{i-1} - tu_i, \quad v_{i+1} = v_{i-1} - tv_i$$

où t est pris de la relation $d_{i+1} = d_{i-1} - td_i$.

Comme $\text{pgcd}(a, b) = d_{k-1}$ on peut prendre $u = u_{k-1}, \quad v = v_{k-1}$.

Programme pour calculer u et v

```
> bezout:=proc(a::integer,b::integer)
> local u0,u1,u2,v0,v1,v2,d0,d1,r,t,i;
> if a<0 then a:=-a;
> else fi;
> if b<0 then b:=-b;
> else fi;
> u0:=1;v0:=0;
> u1:=0;v1:=1;
> d0:=a; d1:=b;
> r:=b;
> i:=0;
> while(d1<>0) do
> i:=i+1;
> t:=iquo( d0,d1 );
> r:=irem( d0,d1 );
> d0:=d1;
> d1:= r;
> u2:=u0-t*u1;
> v2:=v0-t*v1;
> u0:=u1;
> u1:= u2;
> v0:=v1;
> v1:= v2;
> printf("i=%d,%d*%d+%d*%d=%d\n"
> ,i,a,(u0) , b,v0, d0)
> od;
> return d0;
> end proc;
```

```
bezout := proc(a::integer, b::integer)
local u0, u1, u2, v0, v1, v2, d0, d1, r, t, i;
  if a < 0 then a := -a else end if;
  if b < 0 then b := -b else end if;
  u0 := 1;
  v0 := 0;
  u1 := 0;
  v1 := 1;
  d0 := a;
  d1 := b;
  r := b;
  i := 0;
  while d1 <> 0 do
    i := i + 1;
    t := iquo(d0, d1);
    r := irem(d0, d1);
    d0 := d1;
    d1 := r;
    u2 := u0 - t * u1;
    v2 := v0 - t * v1;
    u0 := u1;
    u1 := u2;
    v0 := v1;
    v1 := v2;
    printf("i=%d,%d*%d+%d*%d=%d \n", i, a, u0, b, v0, d0)
  end do;
  return d0
end proc
```

```
> bezout(12,14);
```

```
i=1,12*0+14*1=14

i=2,12*1+14*0=12

i=3,12*-1+14*1=2
```

2

```
> bezout(691,1000);
```

```
i=1,691*0+1000*1=1000

i=2,691*1+1000*0=691

i=3,691*-1+1000*1=309

i=4,691*3+1000*-2=73

i=5,691*-13+1000*9=17

i=6,691*55+1000*-38=5

i=7,691*-178+1000*123=2
```

```
i=8,691*411+1000*-284=1
```

$$1$$

```
> bezout(17,61);
i=1,17*0+61*1=61
i=2,17*1+61*0=17
i=3,17*-3+61*1=10
i=4,17*4+61*-1=7
i=5,17*-7+61*2=3
i=6,17*18+61*-5=1
```

$$1$$

Pour résoudre $ax \equiv 1 \pmod{n}$

on peut simplement utiliser en Maple la commande

```
> 1/a mod n;
```

Sinon, on suppose $\text{pgcd}(a, n) = 1$. Pour résoudre $ax \equiv 1 \pmod{n}$ on trouve x et y tels que $ax+ny = 1$. Alors

$$ax \equiv ax + ny \equiv 1 \pmod{n}.$$

EXEMPLE 3.2.6 *Résoudre* $17x \equiv 1 \pmod{61}$. *Premièrement, on utilise l'algorithme d'Euclide pour trouver* x, y *tels que* $17x + 61y = 1$ *:*

$$\begin{aligned} \overline{61} &= 3 \cdot \overline{17} + \overline{10} && \textit{donc } \overline{10} = \overline{61} - 3 \cdot \overline{17} \\ \overline{17} &= 1 \cdot \overline{10} + \overline{7} && \textit{donc } \overline{7} = -\overline{61} + 4 \cdot \overline{17} \\ \overline{10} &= 1 \cdot \overline{7} + \overline{3} && \textit{donc } \overline{3} = 2 \cdot \overline{61} - 7 \cdot \overline{17} \\ \overline{3} &= 2 \cdot \overline{3} + \overline{1} && \textit{donc } \overline{1} = -5 \cdot \overline{61} + 18 \cdot \overline{17}. \end{aligned}$$

Alors $x = 18$ *est une solution de* $17x \equiv 1 \pmod{61}$.

La même chose se fait facilement en utilisant Maple

```
> restart;
> 1/17 mod 61;
```

$$18$$

```
> 1/2 mod 61;
```

$$31$$

3.3 Sous-groupes

DÉFINITION 3.3.1 *Si* G *est un groupe, un sous-groupe de* G *est une partie* H *de* G *vérifiant les trois conditions suivantes :*

SG1 $e \in H$,
SG2 $\forall x, y \in H, xy \in H$,
SG3 $\forall x \in H, x^{-1} \in H$.

H est alors un groupe pour la loi induite

$$H \times H \to H,\ (h_1, h_2) \mapsto h_1 h_2$$

EXEMPLE 3.3.2 *Si G est un groupe, G et $\{e\}$ sont des sous-groupes de G.*

EXEMPLE 3.3.3 *Si $(H_i)_{i\in I}$ est une famille des sous-groupes d'un groupe G, alors l'intersection $\cap_{i\in I} H_i$ est un sous-groupe de G. En particulier, si X est une partie de G, l'intersection des sous-groupes de G contenant X, est un sous-groupe de G. C'est le plus petit sous-groupe de G contenant X, on l'appelle le sous-groupe de G* engendré par *X. On notera $\langle X\rangle$ le sous-groupe engendré par X.*

EXEMPLE 3.3.4 *Si $\phi : G \to H$ un morphisme de groupes, alors pour tout sous-groupe H' de H, son image inverse dans G, $\phi^{-1}(H') \subset G$ est un sous groupe de G, et pour tout sous-groupe G' de G, son image $\phi(G') \subset H$ est un sous groupe de H. En particulier, l'ensemble*

$$\mathrm{Ker}(\phi) = \phi^{-1}(e) \subset G = \{x \in G \mid \phi(x) = e\}$$

est un sous-groupe de G appelé le noyau *de ϕ. L'image de ϕ, notée $\mathrm{Im}(\phi)$, est un sous-groupe de H.*

THÉORÈME 3.3.5 *Si G est un groupe, et g est un élément de G alors il existe un seul morphisme $\phi : \mathbb{Z} \to G$ déterminé par la formule*

$$k \mapsto g^k \text{ pour } k \in \mathbb{Z}.$$

L'image de ϕ, notée $\mathrm{Im}(\phi)$, est le sous-groupe $H = \langle g\rangle$ de G, engendré par g.

PREUVE. Il suffit de remarquer que g^k est définie de la façon suivante

$$g^0 = e, \forall k \in \mathbb{N}, g^{k+1} = g^k g, \text{ et } g^{-k} = (g^k)^{-1},$$

donc on a un morphisme déterminé par la formule

$$\phi : k \mapsto g^k \text{ pour } k \in \mathbb{Z}$$

car $\phi(k+l) = g^{k+l} = g^k g^l = \phi(k)\phi(l)$.

THÉORÈME 3.3.6 *Soit I un sous-groupe du groupe additif $\mathbb{Z}$. Alors tout sous-groupe de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$, pour un élément n de $\mathbb{Z}$.*

PREUVE. Si I est distinct du sous-groupe $\{0\}$, alors I contient un élément non-nul et, contenant aussi son opposé, un élément strictement positif. Soit n le plus petit élément strictement positif de I. Soit i un élément quelconque de I. La division euclidienne de i par n s'écrit $i = nq + r$ avec $0 \leq r < n$. Mais $r = i - nq$ appartient également à I. Par conséquance, par minimalité de n, on a $r = 0$. Donc $i \in n\mathbb{Z}$. Réciproquement, tout élément de $n\mathbb{Z}$ est dans I. En notant que $\{0\} = 0\mathbb{Z}$, on obtient que tout sous-groupe de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$, pour un élément n de $\mathbb{Z}$.

COROLLAIRE 3.3.7 *Soit $G = \langle g\rangle$ un groupe cyclique d'ordre N. Alors tout sous-groupe H de G est cyclique.*

PREUVE. On utilise le morphisme $\phi : \mathbb{Z} \to G$ déterminé par la formule

$$k \mapsto g^k \text{ pour } k \in \mathbb{Z}.$$

Alors ϕ est *surjectif* parce que G est engendré par g. On considère l'image inverse du sous-groupe $H \subset G$: $\phi^{-1}(H) \subset \phi^{-1}(G) = \mathbb{Z}$.

Selon théorème 3.3.6, tout sous-groupe de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$, pour un élément n de $\mathbb{Z}$. Ceci implique que $H = \phi(I) = \langle g^n\rangle$.

3.4 Classes à gauche, à droite

Définition 3.4.1 *Soit G groupe et H un sous-groupe de G. Si $g \in G$, l'ensemble*

$$gH = \{gh \mid h \in H\} \text{ (resp. } Hg = \{hg \mid h \in H)\}$$

est appelé classe à gauche (resp. à droite) de g pour H. On note G/H (resp. $H\backslash G$) l'ensemble des classes à gauche (resp. à droite) de G pour H.

Notons que si a et b sont des éléments de G, alors on a une bijection

$$\begin{aligned} aH &\to bH \\ g &\mapsto ba^{-1}g \end{aligned}$$

De même façon on a une bijection

$$\begin{aligned} aH &\to Ha^{-1} \\ g &\mapsto g^{-1} \end{aligned}$$

En particulier, toutes les classes ont le même cardinal, à savoir, le cardinal du sous-groupe H. En outre cela défini une bijection

$$\begin{aligned} G/H &\to H\backslash G \\ aH &\mapsto Ha^{-1} \end{aligned}$$

Définition 3.4.2 *Soit G groupe et H un sous-groupe de G. Si l'ensemble G/H ou $H\backslash G$ des classes à gauche (resp. à droite) est fini, alors tous ces deus ensembles sont finis et de même cardinal, qu'on appèle* indice *de H dans G. On le note $(G : H)$.*

Nous avons montré la propriété suivante

Proposition 3.4.3 *Si G est un groupe fini et H est un sous-groupe de G, alors*

$$\sharp G = \sharp H \cdot (G : H).$$

En particulier, le cardinal du sous-groupe divise le cardinal de G.

3.5 Sous-groupes distingués, groupes quotient

Soit $\phi : G \to H$ un morphisme de groupes, alors pour tout x de $\mathrm{Ker}(\phi)$ et tout g de G on a

$$\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g^{-1}) = \phi(g)\phi(g^{-1}) = e.$$

Par conséquant, gxg^{-1} appartient également au noyau de ϕ. Ceci amène à la définition suivante :

Définition 3.5.1 *Soit G groupe et H un sous-groupe de G. On dit que H est* distingué *dans G, et on note $H \triangleleft G$ si et seulement si*

$$\forall g \in G, \forall h \in H, ghg^{-1} \in H.$$

Nous venons de voir que si ϕ est un morphisme, son noyau est distingué. Montrons qu'inversement tout sous-groupe distingué est le noyau d'un morphisme.

Définition 3.5.2 *Si H est un sous-groupe distingué de G, alors il existe sur G/H une unique loi de groupe de sorte que la projection canonique*

$$\phi : G \to G/H, g \mapsto gH$$

soit un morphisme de groupes. On dit alors que G/H est le groupe-quotient *de G par H.*

Exemple 3.5.3 *Si G est un groupe abélien, alors tout sous-groupe H de G est distingué. En particulier, le gous-groupe $n\mathbb{Z}$ est distingué dans $\mathbb{Z}$. On retrouve ainsi une addition dans $\mathbb{Z}/n\mathbb{Z}$.*

Exemple 3.5.4 *Si $\phi : G \to H$ est un morphisme de groupes et H' un sous-groupe distingué de H, alors $\phi^{-1}(H')$ est un sous-groupe distingué de G.*

Preuve : en exercice obligatoire.

Théorème 3.5.5 (Sur l'isomorphime) *Si $\phi : G \to H$ est un morphisme de groupes, et $K = \mathrm{Ker}(\phi)$ son noyau, $K \triangleleft G$, alors il existe un unique isomorphisme de groupes $\overline{\phi} : G/K \to \mathrm{Im}(\phi)$ tel que ϕ coïncide avec la composée*

$$G \xrightarrow{\pi} G/K \xrightarrow{\overline{\phi}} \mathrm{Im}(\phi) \xhookrightarrow{j} H$$

où π désigne la projection canonique, et j l'injection canonique.

Théorème 3.5.6 (Sur l'isomorphime des groupes monogènes) *Si $G = \langle g \rangle$ est un groupe monogène, alors seulement deux cas sont possibles*

(i) G est infini et isomorphe à $\mathbb{Z}$;

(ii) G est fini d'ordre N et isomorphe à $\mathbb{Z}/N\mathbb{Z}$.

Preuve. On considère le morphisme de groupe $\phi : \mathbb{Z} \to G$, qui est surjectif par l'hypothèse. Soit $I = \mathrm{Ker}(\phi) \subset \mathbb{Z}$ son noyau, alors selon théorème 3.5.5, il existe un isomorphisme de groupes $\overline{\phi} : \mathbb{Z}/I \to \mathrm{Im}(\phi) = G$. Alors tout sous-groupe de $\mathbb{Z}$ est de la forme $N\mathbb{Z}$, pour un élément N de $\mathbb{Z}$.

Si $N = 0$, G est infini et isomorphe à $\mathbb{Z}$;

Si $N \neq 0$, G est fini d'ordre N et isomorphe à $\mathbb{Z}/N\mathbb{Z}$.

3.6 Ordre d'un élément, théorème de Lagrange

Définition 3.6.1 *Soit g un élément d'un groupe G. S'il existe un entier strictement positif n tel que $g^n = e$, alors on peut choisir n minimal avec cette propriété. On dit alors que g est un élément d'ordre n, et on le note $n = \mathrm{ord}(g)$.*

S'il n'existe pas d'entier strictement positif n tel que $g^n = e$, on dit que g est un élément d'ordre infini.

Proposition 3.6.2 *Soit g est un élément d'ordre N d'un groupe G, $N = \mathrm{ord}(g)$.*

Alors $N = \mathrm{ord}(g)$ coïncide avec l'ordre du sous-groupe $\langle g \rangle$ engendré par g.

Preuve. Selon le théorème 3.5.6 sur les groupes monogènes, il existe un isomorphisme $\overline{\phi} : \mathbb{Z} \to \langle g \rangle = \mathrm{Im}(\phi)$, où N est le plus petit nombre positif tel que $N \in \mathrm{Ker}\phi$, i.e. $g^N = e$. On voit donc que N coïncide avec l'ordre d'élément g, CQFD.

Théorème 3.6.3 (Lagrange) (voir Proposition 3.4.3)

Si H un sous-groupe d'un groupe fini G, alors $|H|$ divise $|G|$.

De plus, $|G| = |H| \cdot |G/H|$.

Corollaire 3.6.4 *Soit g est un élément d'ordre n d'un groupe fini G, alors $\mathrm{ord}(g)$ divise $|G|$.*

De plus, $|G| = |G/\langle g \rangle| \cdot \mathrm{ord}(g)$

EXERCICE 3.6.5 *Montrer que pour tout diviseur d d'un nombre entier positif N, il existe un élément d'ordre d dans le groupe cyclique $\mathbb{Z}/N\mathbb{Z}$.*

EXERCICE 3.6.6 *Trouver tous les ordres d'éléments dans le groupe multiplicatif $(\mathbb{Z}/61\mathbb{Z})^\times$*

EXERCICE 3.6.7 *Trouver l'ordre des éléments $\overline{17}$, $\overline{2}$ et $\overline{3}$ du groupe multiplicatif $(\mathbb{Z}/61\mathbb{Z})^\times$*

```
> restart;
> 5 &^ 1000 mod 100;
                                    25
> 17&^ 20 mod 61;
                                    13
> 17&^ 30 mod 61;
                                    60
> 17&^ 12 mod 61;
                                    20
> 2&^ 20 mod 61;
                                    47
> 2&^ 30 mod 61;
                                    60
> 2&^ 12 mod 61;
                                     9
> 3&^ 20 mod 61;
                                     1
> 3&^ 10 mod 61;
                                     1
> 3&^ 5 mod 61;
                                    60
> 3&^ 2 mod 61;
                                     9
```

Réponse : $\mathrm{ord}(\overline{17}) = 60$, $\mathrm{ord}(\overline{2}) = 60$ et $\mathrm{ord}(\overline{3}) = 10$.

EXERCICES

3.1 Trouver pour tout diviseur d d'un nombre entier positif N, tous les éléments d'ordre d dans le groupe cyclique $\mathbb{Z}/N\mathbb{Z}$.

3.2 Trouver tous les éléments d'ordre maximal dans le groupe multiplicatif $(\mathbb{Z}/61\mathbb{Z})^\times$

3.3 Les groupes multiplicatifs $(\mathbb{Z}/8\mathbb{Z})^\times$ et $(\mathbb{Z}/18\mathbb{Z})^\times$ sont-ils cycliques ?

3.4 Trouver l'ordre des éléments $\overline{5}$ et $\overline{7}$ du groupe multiplicatif $(\mathbb{Z}/61\mathbb{Z})^\times$

3.5 Trouver tous les éléments d'ordre maximal dans les groupes de permutations $\mathfrak{S}_3$ et $\mathfrak{S}_4$.

Cours N°3. Jeudi le 16 octobre 2003

4 Rappels sur la notion d'anneau, exemples

4.1 Structure d'anneau et idéaux

DÉFINITION 4.1.1 *Un anneau est un groupe abélien A muni d'une loi interne*

$$A \times A \to A, \quad (x, y) \mapsto xy = x \cdot y$$

appelé produit ou multiplication, qui est associative

An1 $\forall x, y, z \in A, x(yz) = (xy)z$,

et distributive à droit et à gauche par rapport à l'addition :

An2 $\forall x, y, z \in A, x(y + z) = xy + xz$,

An3 $\forall x, y, z \in A, (y + z)x = yx + zx$,

On prendra également la convention que tout anneau est unifère, c'est à dire que la multiplication est munie d'un élément neutre 1 :

An3 $\forall x \in A, 1x = x1 = x$.

L'anneau est dit commutatif si la loi de multiplication est commutative :

Comm. $\forall x, y \in A, xy = yx$.

DÉFINITION 4.1.2 *Un morphisme d'anneau $\varphi : A \to B$ est une application telle que*

MorAn $\forall x, y, z \in A, \varphi(xy + z) = \varphi(x)\varphi(y) + \varphi(z) \in A, \varphi(1_A) = 1_B$

SAn *Une partie $A \subset B$ est dit un sous-anneau, si l'inclusion $A \hookrightarrow B$ est un morphisme d'anneau.*

EXEMPLE. On pose $B = \mathbb{Z} \times \mathbb{Z} = \{(x_1, x_2) \mid x_1, x_2 \in \mathbb{Z}\}$, alors $A = \{0\} \times \mathbb{Z}$ est un anneau, mais non un sous-anneau de B.

DÉFINITION 4.1.3 *Soit A un anneau commutatif. Une partie $I \subset A$ est dit un idéal si c'est un sous-groupe additif pour l'addition, stable par la multiplication externe (par un élément quelconque $y \in A$*

Idéal $\forall x \in I, \forall a \in A, ax \in I$.

Opérations sur les idéaux

DÉFINITION 4.1.4

(a) Soient I, J deux idéaux de de A. Leur somme

$$I + J = \{x + y \mid x \in I, y \in J\}$$

est le plus petit idéal de A contenant I et J.

La somme d'une famille d'idéaux $(I_\alpha)_{\alpha \in \Gamma}$ *est formée par toutes les sommes finies*

$$\sum_{\alpha \in \Gamma} I_\alpha = \left\{ \sum_{\alpha \in \Gamma} x_\alpha, x_\alpha \in I_\alpha \right\}$$

où $x_\alpha = 0$ sauf un nombre fini de $\alpha \in \Gamma$.

(b) L'intersection ensembliste

$$\bigcap_{\alpha \in \Gamma} I_\alpha$$

d'une famille d'idéaux $(I_\alpha)_{\alpha\in\Gamma}$ *est toujours un idéal de* A.

(c) Soit X *une partie d'un anneau* A. *L'intersection de tous les idéaux de* A, *contenants* X, *est dit l'idéal* engendré par X

(d) Le produit

$$I_1 \cdot I_2 \cdot \ldots \cdot I_n$$

d'un nombre fini d'idéaux est l'idéal engendré par

$$\{x_1 \cdot x_2 \cdot \ldots \cdot x_n \mid x_1 \in I_1, x_2 \in I_1, \cdots, x_n \in I_n\}$$

En particulier, l'idéal I^n est engendré par

$$\{x_1 \cdot x_2 \cdot \ldots \cdot x_n \mid x_1, x_2 \in I_1, \cdots, x_n \in I\}$$

Exemple.

a) Si $A = \mathbb{Z}$, $I = (m)$, $J = (n)$, alors

$$I + J = (\text{pgcd}(m, n)), I \cap J = (\text{ppcm}(m, n)), I \cdot J = (mn).$$

Remarque.

L'idéal, engendré par une famille x_α, coïncide avec la somme

$$\sum_{\alpha\in\Gamma}(x_\alpha)$$

de tous les idéaux principaux $(x_\alpha) = x_\alpha A$.

Remarque. Montrer en exercice que l'union d'une famille d'idéaux $(I_\alpha)_{\alpha\in\Gamma}$ n'est pas un idéal en général, mais c'est le cas si les idéaux I_α sont totalement ordonnés par l'inclusion :

$$\forall \alpha, \beta, \text{ soit } I_\alpha \subset I_\beta, \text{ soit } I_\beta \subset I_\alpha.$$

4.2 Anneau quotient

Définition 4.2.1 *Soit* A *un anneau commutatif,* $I \subset A$ *un idéal de* A. *Alors il existe sur le groupe quotient additif* A/I *une unique structure d'anneau telle que la projection canonique* $\pi : A \to A/I$ *est un morphisme d'anneaux.*

Proposition 4.2.2

(a) Soit A *un anneau commutatif,* $I \subset A$ *un idéal de* A. *Alors il existe une bijection entre l'ensemble*

$$\{J \subset A \mid J \supset I\}$$

d'idéaux contenants I, *et l'ensemble*

$$\left\{\overline{J} \subset A/I\right\}$$

d'idéaux de A/I, *donnée par* $J = \pi :^{-1} (\overline{J})$, *où* $\pi : A \to A/I$ *est la projection canonique.*

(b) Soit $\psi : A \to B$ *un morphisme d'anneaux, alors* $I = \text{Ker}\psi := \psi^{-1}(0)$ *est un idéal de* A, $\psi(A) = C$ *est un sous-anneau de* B, *et il y a un isomorphisme d'anneaux*

$$\overline{\psi} : A/I \xrightarrow{\sim} C.$$

Notations.

On écrit

$$x \equiv y \bmod I \iff x - y \in I.$$

Diviseurs de zéro, éléments nilpotents et unités

DÉFINITION 4.2.3

(a) Un $x \in A\backslash\{0\}$ est dit diviseur de zéro*, s'il existe un $y \in A\backslash\{0\}$ tel que $xy = 0$. Un anneau $A \neq \{0\}$ sans diviseurs de zéro est dit* intègre*.*

(b) Un élément $x \in A\backslash\{0\}$ est dit nilpotent*, si $x^n = 0$ pour un $n \geq 1$.*

(c) Un élément $x \in A$ esi dit inversible *(ou une* unité*) de A s'il existe $y \in A, xy = 1$. On notera $x \in A^\times$.*

DÉFINITION 4.2.4 *Un corps est un anneau commutatif A, non réduit à $\{0\}$ dans lequel tout élément non-nul est inversible :*

Corps $\forall x \in A, x \neq 0, \exists y \in A, xy = 1$

PROPOSITION 4.2.5

(a) Soit A un corps, alors A est un anneau intégre.

(b) Soit A un corps, I un idéal de A. Alors soit $I = \{0\}$ soit $I = A$.

4.3 Idéaux premiers

DÉFINITION 4.3.1

(a) Un idéal $I \neq A$ est dit premier*, si*

$$\forall x, y \in A, x \cdot y \in I \Longleftrightarrow x \in I \text{ ou } y \in I,$$

i.e. l'anneau quotient A/I est intègre.

(b) Un idéal $I \neq A$ est dit maximal*, si*

$$\forall \text{ idéal } J \subset A, I \subset J \Rightarrow I = J, \text{ ou } J = A$$

PROPOSITION 4.3.2

(a) Un idéal $I \neq A$ est dit maximal*, si et seulement si A/I est un corps*

(b) Tout idéal maximal est premier.

PREUVE (a) On suppose I maximal. Si $x \notin I$, on considère l'idéal (x, I) engendré par x et I. Alors $(x, I) \neq I$ donc $(x, I) = A$; ceci dit, il existe $a \in A$ et $b \in I$ tels que $ax + b = 1$; ceci dit, $\overline{ax} = \overline{1}$ dans A/I.

Réciproquement, si A/I est un corps, les seuls idéaux de A/I sont $\{0\}$ et A/I. Par la proposition 4.2.2, a), il existe une bijection entre l'ensemble

$$\{J \subset A \mid J \supset I\}$$

d'idéaux contenants I, et l'ensemble

$$\left\{\overline{J} \subset A/I\right\}$$

d'idéaux de A/I. Donc il n'y a pas d'idéaux stricts intermédiaires entre I et A, i.e. I est maximal.

(b) Un corps est toujours un anneau intègre, donc I est premier.

EXEMPLE.

a) Dans l'anneau $A = \mathbb{C}[X, Y]$ l'idéal $I = (X, Y)$ est maxmal, $A/I \xrightarrow{\sim} \mathbb{C}$.

L'idéal $J = (X)$ n'est pas maxmal, mais premier :$A/J \xrightarrow{\sim} \mathbb{C}[Y]$.

b) Trouver tous les idéaux maximaux dans l'anneau $A = \mathbb{Z}[X]$.

L'idéal $J = (p)$ n'est pas maxmal, mais premier :$A/J \xrightarrow{\sim} \mathbb{F}_p[X]$.

4.4 Divisibilité dans les anneaux

DÉFINITION 4.4.1 *Soit A un anneau commutatif.*

(a) Si a et $b \in A$, on dit que a divise *b et on note $a|b$ s'il existe un $c \in A$ tel que $b = ac$. On dit également que b est un* multiple *de a ou a un* diviseur *de b. On note $(a) = aA$ l'insemble des multiples de a. C'est un idéal de A engendré par a.*

(b) Soit A un anneau intègre*. Deux éléments a et $b \in A$ sont dits* associés *si et seulement s'ils vérifient une des conditions équivanentes suivantes :*

(i) $\exists u \in A^\times, b = ua$
(ii) $a|b$ *et* $b|a$
(iii) $(a) = (b)$

On notera dans ce paragraphe $a \sim b$ (c'est une relation d'équivalence).

DÉFINITION 4.4.2 *Un élément $a \in A$ est dit* irréductible*, si et seulement si il vérifie les deux conditions suivantes :*

Irr1. $a \notin A^\times$
Irr2. *Si $a = bc$ avec $a, b \in A$ alors $a \in A^\times$ ou $b \in A^\times$.*

EXEMPLE. Les éléments irréductibles de $\mathbb{Z}$ sont les éléments de la forme p ou $-p$ avec p un nombre premier parce que $\mathbb{Z}^\times = \{\pm 1\}$.

PROPOSITION 4.4.3 *Soit $p \in A\backslash\{0\}$. Si (p) est premier alors p est irréductible. La réciproque est fausse en générale.*

DÉFINITION 4.4.4 *Soit A un anneau commutatif intègre, I un ensemble et $(a_i)_{i\in I}$ une famille d'éléments de A.*

(i) On dit que $d \in A$ est un pgcd de la famille $(a_i)_{i\in I}$, $d = \mathrm{pgcd}(a_i)_{i\in I}$, si

$$\forall i \in I, d|a_i \text{ et } \forall r \in A, \forall i \in I, r|a_i \Rightarrow r|d$$

(ii) On dit que $m \in A$ est un ppcm de la famille $(a_i)_{i\in I}$, $m = \mathrm{ppcm}(a_i)_{i\in I}$, si

$$\forall i \in I, a_i|m \text{ et } \forall r \in A, \forall i \in I, a_i|r \Rightarrow m|r$$

EXEMPLE 4.4.5 *Le pgcd et ppcm n'existe pas toujours dans un anneau commutatif. Un exemple connu est donné par l'anneau $\mathbb{Z}[\sqrt{-5}]$ dans lequel il existe essentiellement différentes factorisations en éléments premiers :*

$$2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}).$$

On pose $a = 2$ et $b = 1 + \sqrt{-5}$. Montrer que $\mathrm{pgcd}(a, b)$ et $\mathrm{ppcm}(a, b)$ n'existe pas dans A.

REMARQUE. Si $d = \mathrm{pgcd}(a_i)_{i\in I}$ et $m = \mathrm{ppcm}(a_i)_{i\in I}$ existent, il ne sont en fait pas uniques. Seules leurs classes d'équivalence dans $A/\sim$ le sont.

4.5 Anneaux euclidiens et anneaux principaux

La notion de division sur les polynômes et les entiers conduit à la notion d'anneau euclidien.

DÉFINITION 4.5.1 *Un anneau intègre A est dit* euclidien *s'il existe une application $\phi : A \to \mathbb{N}$ appelée* stathme *telle que*

$$\forall a \in A\backslash\{0\} \forall b \in A, \exists (q,r) \in A^2, b = aq + r \text{ avec } r = 0 \text{ ou } \phi(r) < \phi(a)$$

EXEMPLE. L'anneau des entiers $\mathbb{Z}$ est euclidien pour la valeur absolue.

EXERCICE. Montrer que les anneaux $\mathbb{Z}[i]$ et $\mathbb{Z}[j]$ sont euclidiens pour le carré de la valeur absolue complexe.

DÉFINITION 4.5.2 *Un anneau intègre A est dit* principal *si tout idéal I de A est princapal, c'est à dire, il existe un $a \in A$, tel que $I = (a)$.*

THÉORÈME 4.5.3 *Tout anneau A euclidien est principal.*

PREUVE. Soit A un anneau euclidien et I un idéal de A. Si $I \neq \{0\}$, il existe un élément non nul dans I. On choisit un élément x de I tel que $\phi(x)$ soit minimal. Alors $I = (x)$. En effet, pour tout $y \in I$, on écrit $y = xq + r$ avec $r = 0$ ou $\phi(r) < \phi(x)$. Comme $r = y - xq$, $r \in I$ et par minimalité de $\phi(x)$, $r = 0$. Donc $y \in (x)$, CQFD

PROPOSITION 4.5.4 *Soit A un anneau principal. Les assertions suivantes sont équivalentes :*
(i) $\mathfrak{a}$ est un idéal maximal non nul de A ;
(ii) $\mathfrak{a}$ est un idéal premier non nul de A ;
(iii) il existe un élément p irréductible de A tel que $\mathfrak{a} = (p)$.

PREUVE. *(i)⇒(ii) Puisqu'un idéal maximal est premier.*
(ii)⇒(iii) Comme A est principal, il existe p tel que $\mathfrak{a} = (p)$ mais comme (p) est premier, p est irréductible.
(iii)⇒(i) Soit p irréductible et $\mathfrak{a} = (p)$. Par l'hypothèse, $p \notin A^\times$, donc $\mathfrak{a} \neq A$. Soit $\mathfrak{b}$ tel que $\mathfrak{a} \subset \mathfrak{b}$. Comme A est principal, $\mathfrak{b} = (q)$. Donc $q|p$, si $\mathfrak{a} \neq \mathfrak{b}$, alors q et p ne sont pas associés. Donc $q \in A^\times$, et $\mathfrak{b} = A$.

COROLLAIRE 4.5.5 (LEMME D'EUCLIDE) *Soit A un anneau principal, p un élément irréductible dans A. Alors*

$$p|ab \Rightarrow (p|a \text{ ou } p|b).$$

PROPOSITION 4.5.6 *Soit A un anneau principal, alors toute famille $(a_i)_{i\in I}$ d'éléments de A admet un pgcd et ppcm.*

PREUVE. Le pgcd est donné comme un générateur de l'idéal $\sum_{i\in I}(a_i)$ et le ppcm comme générateur de l'idéal $\bigcap_{i\in I}(a_i)$.

PROPOSITION 4.5.7 (BEZOUT) *Si A est un anneau principal et $a_1, \cdots, a_n \in A$, alors il existe $b_1, \cdots, b_n \in A$ tels que*

$$a_1b_1 + \cdots + a_nb_n = \text{pgcd}(a_1, \cdots, a_n)$$

PREUVE. Le pgcd est un générateur de l'idéal $(a_1, \cdots, a_n)$, donc il existe $b_1, \cdots, b_n \in A$ tels que

$$a_1b_1 + \cdots + a_nb_n = \text{pgcd}(a_1, \cdots, a_n).$$

Définition 4.5.8 *Si A est un anneau principal et $a_1, \cdots, a_n \in A$, Si* $\mathrm{pgcd}(a_1, \cdots, a_n) = 1$ *alors on dit que $a_1, \cdots, a_n$ sont* premiers entre eux. *Dans ce cas il existe $b_1, \cdots, b_n \in A$ tels que*

$$a_1 b_1 + \cdots + a_n b_n = 1$$

Proposition 4.5.9 (Lemme de Gauss) *Soit A est un anneau principal et $b, c \in A$ deux éléments premiers entre eux. Si $c|ab$, alors $c|a$.*

Preuve. Par le théorème de Bezout, il existe u, v tels que $bu + cv = 1$. Comme $c|ab$ par l'hypothèse,

$$c|a(bu + cv) = abu + acv = a, \qquad \square$$

ceci implique que $c|a$.

4.6 Décomposition en facteurs premiers

Définition 4.6.1 *Un anneau intègre A est dit* factoriel *si et seulement si il vérifie les conditions suivantes :*
Existence. *Pour tout élément non nul a de A il existe un élément inversible $u \in A^\times$ et des éléments irréductibles $p_1, \cdots, p_m$ de A tels que*

$$a = u p_1 \cdot \ldots \cdot p_m$$

(il ce peut que $m = 0$, dans ce cas $a \in A^\times$).
Unicité. *Soient m, n, $p_1, \cdots, p_m$ et $q_1, \cdots, q_m$ des éléments irréductibles de A et $u, v \in A^\times$ des éléments inversibles de A tels que*

$$u p_1 \cdot \ldots \cdot p_m = v q_1 \cdot \ldots \cdot q_n,$$

alors $m = n$ et il existe une permutation $\sigma \in \mathfrak{S}_n$ telle que $q_i \sim p_{\sigma(i)}$ pour $i = 1, \cdots n$.

Théorème 4.6.2 *Tout anneau A principal est factoriel.*

Preuve. Existence. On raisonne par l'absurde : soit a_0 un élément de $A \backslash \{0\}$, non-inversible, qui ne s'écrit pas comme produit d'éléments irréductibles. En particulier, a_0 n'est pas irréductible et on peut écrire : $a_0 = a_1 a_1'$ avec a_1 et a_1' non inversibles. Si ces deux éléments sont produit d'irréductibles, alors il en est de même de a_0. Quitte à échanger a_1 et a_1', on peut supposer que a_1 n'est pas produit d'irréductibles. En itérant, on obtient une suite infinie $a_0, a_1, \cdots, a_n \cdots$ d'éléménts tels que

$$(a_0) \subsetneq (a_1) \subsetneq (a_n) \subsetneq \cdots \subsetneq \cdots$$

La réunion $I = \bigcup_{n=0}^{\infty}$ est un idéal de A. En effet $0 \in I$ et si b_1 et b_2 appartiennent à I, il existe n_1 et n_2 tels que $b_1 \in a_{n_1}$ et $b_2 \in a_{n_2}$. Soit $n = \sup(n_1, n_2)$, alors $b_1 - b_2 \in (a_n)$ donc I est un sous groupe de A et si b appartient à I et a à A il existe n tel que $b \in\in (a_n)$ et $ab \in (a_n) \subset I$. Comme A est principal, $I = (a)$ pour un $a \in A$. Mais comme $a \in I$, il existe n tel que $a \in (a_n)$ donc

$$(a_n) \subsetneq (a_{n+1}) \subsetneq (a_n) \subset I = (a) \subset (a_n),$$

ce que est absurde.

Unicité. Si on a une égalité de la forme

$$u p_1 \cdot \ldots \cdot p_m = v q_1 \cdot \ldots \cdot q_n,$$

avec $p_1, \cdots, p_m$ et $q_1, \cdots, q_m$ des éléments irréductibles, et $u, v \in A^\times$ des éléments inversibles de A, on peut supposer que $m \geq n$. On procède alors par récurrence sur m. Si $m = 0$, alors $n = 0$ et le résultat

annoncé est vrai. Mais, par le lemme d'Euclide (Corollaire 4.5.5, p_1 divise v ou l'un des q_i. Comme v est inversible, si $p_1|v$ alors p_1 est inversible ce que contredi le fait que p_1 soit irréductible. On a

$$p_1|q_1 \cdot \ldots \cdot q_s.$$

Donc p_1 divise l'un des q_i.

Quitte à échanger les q_i, on peut supposer que $p_1|q_1$. Comme le nombre q_1 est premier, on obtient $p_1 = wq_1$ avec $w \in A^\times$, d'où

$$p_2 \cdot \ldots \cdot p_m = (vw)q_2 \cdot \ldots \cdot q_n$$

(après la simplification), et il reste à appliquer l'hypothèse de récurrence au produit $p_2 \cdot \ldots \cdot p_m$ de $m-1$ facteurs irréductibles.

Exercices

4.1 Le pgcd et ppcm n'existe pas toujours dans un anneau commutatif. Un exemple connu est donné par l'anneau $\mathbb{Z}[\sqrt{-5}]$ dans lequel il existe essentiellement différentes factorisations en éléments premiers :

$$2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}).$$

On pose $a = 2$ et $b = 1 + \sqrt{-5}$. Montrer que $\text{pgcd}(a, b)$ et $\text{ppcm}(a, b)$ n'existe pas dans A.

4.2 Trouver tous les diviseurs de zéro dans les anneaux

$$\mathbb{Z}/100\mathbb{Z}, \mathbb{Z}/72\mathbb{Z}, \mathbb{Z}/p^n\mathbb{Z}.$$

4.3 Trouver tous les éléments nilpotents dans les anneaux

$$\mathbb{Z}/100\mathbb{Z}, \mathbb{Z}/72\mathbb{Z}, \mathbb{Z}/p^n\mathbb{Z}.$$

4.4 Trouver tous les éléments inversibles dans les anneau

$$\mathbb{Z}/100\mathbb{Z}, \mathbb{Z}/72\mathbb{Z}, \mathbb{Z}/p^n\mathbb{Z}.$$

4.5 Montrer qu'un anneau fini A est intègre si et seulement s'il est un corps.

4.6 Montrer que les anneaux $\mathbb{Z}[i]$ et $\mathbb{Z}[j]$ sont euclidiens pour le carré de la valeur absolue complexe.

4.7 Trouver tous les éléments inversibles dans les anneau $\mathbb{Z}[i]$ et $\mathbb{Z}[j]$.

4.8 Décrire tous les éléments irréductibles dans les anneau $\mathbb{Z}[i]$ et $\mathbb{Z}[j]$.

4.9 Montrer que l'anneau des nombres décimaux

$$\mathcal{O} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z}, b = 10^k, k \in \mathbb{N} \right\}$$

est un anneau euclidien.

4.10 Montrer que tout corps est un anneau euclidien.

5 Théorème des restes chinois

5.1 Théorème des restes dans les anneaux principaux

Commençons par énoncer un résultat préliminaire :

Proposition 5.1.1 *Si A est un anneau principal et $a_1, \cdots, a_n$ des éléments premiers entre eux deux-à-deux, alors*

$$\text{ppcm}(a_1, \cdots, a_n) = \prod_{i=1}^{n} a_i.$$

LEMME 5.1.2 *Soit A un anneau principal. Si b est premier avec chacun des $a_1, \cdots, a_n$, alors b est premier avec $a_1 \cdot \ldots \cdot a_n$.*

PREUVE du lemme. On procède par récurrence. L'énoncé est vrai si $n = 1$. Montrons le pour $n = 2$. Par le théorème de Bezout, comme b est premier avec a_1 et a_2, il existe des éléments x_1, x_2, y_1, y_2 de A tels que

$$1 = x_1 b + y_1 a_1, \text{ et } 1 = x_2 b + y_2 a_2.$$

Par conséquant,

$$1 = (x_1 b + y_1 a_1)(x_2 b + y_2 a_2) = (x_1 x_2 b + y_1 a_1 x_2 + x_1 y_2 a_2) b + y_1 y_2 a_1 a_2,$$

ce que implique le résultat dans ce cas. Si le résultat est vrai pour $n-1$ par hypothèse de récurrence, b est premier avec $a_1 \cdot \ldots \cdot a_{n-1}$ et a_n. Donc, en utilisant $n = 2$, on obtient que b est premier avec le produit $a_1 \cdot \ldots \cdot a_n$.

PREUVE de la proposition. On montre la proposition par récurrence. Elle est vraie pour $n = 1$. Si $n = 2$, comme

$$a_1 | \frac{\text{ppcm}(a_1, a_2)}{a_2} \times a_2,$$

en appliquant le lemme de Gauss, a_1 divise $\frac{\text{ppcm}(a_1,a_2)}{a_2}$ et donc $a_1 a_2 | \text{ppcm}(a_1, a_2)$. Enfin pour la récurrence on utilise l'assertion qui précède et l'égalité

$$\text{ppcm}(a_1, \cdots, a_n) = \text{ppcm}(\text{ppcm}(a_1, \cdots, a_{n-1}, a_n).$$

THÉORÈME 5.1.3 (THÉORÈME DES RESTES) *Si A est un anneau principal et $a_1, \cdots, a_n$ des éléments premiers entre eux deux-à-deux, alors*

$$A/(a_1 \cdot \ldots \cdot a_n) \xrightarrow{\sim} \prod_{i=1}^{n} A/(a_i).$$

PREUVE du théorème. On considère l'application

$$A \to \prod_{i=1}^{n} A/(a_i),$$

produit des projections canoniques. Son noyau est $\bigcap_{i=1}^{n}(a_i)$ qui par la proposition précédente coïncide avec $\prod_{i=1}^{n}(a_i)$. On obtient donc un morphisme injectif

$$A/(a_1 \cdot \ldots \cdot a_n) \to \prod_{i=1}^{n} A/(a_i).$$

Il reste donc à montrer que cette application est surjective. Cela revient donc à montrer que, sous les hypothèses du théorème, pour toute famille $(x_1, \cdots, x_n)$ de A^n, il existe x dans A tel que $a_i | x - x_i$ pour tout i entre 1 et n. Là encore, nous allons procéder par récurrence. Pour $n = 1$, le résultat est vrai. Pour $n = 2$, en utilisant Bezout, on peur écrire $1 = a_1 b_1 + a_2 b_2$, avec b_1 et b_2 des éléments de A. On pose $x = a_1 b_1 x_2 + a_2 b_2 x_1$. On obtient

$$x - x_1 = a_1 b_1 (x_2 - x_1) \text{ et } x - x_2 = a_2 b_2 (x_1 - x_2).$$

Donc x convient.

Si le résultat est vrai pour $n-1$, il existe y tel que $a_i|y-x_i$ pour $1 \leq i \leq n-1$, et en utilisant le cas $n=2$, il existe un élément x de A tel que

$$\prod_{i=1}^{n-1} a_i|x-y \text{ et } a_n|x_n-y.$$

Par conséquant $a_i|y-x_i$ pour $1 \leq i \leq n$, CQFD.

Cours N°4. Jeudi le 23 octobre 2003

Rappels : théorème des restes dans les anneaux principaux

THÉORÈME DES RESTES 5.1.3. Si A est un anneau principal et $a_1, \cdots, a_n$ des éléments premiers entre eux deux-à-deux, alors

$$A/(a_1 \cdot \ldots \cdot a_n) \xrightarrow{\sim} \prod_{i=1}^{n} A/(a_i).$$

REMARQUE 5.1.4 (THÉORÈME DE BEZOUT : UNE FORME EXPLICITE) *Si A est un anneau principal et $a_1, \cdots, a_n$ des éléments premiers entre eux deux-à-deux, alors on peut explicitement donner un $x \in A$ tel que pour toute collection de classes $x_i \bmod a_i = x_i + (a_i)$, $x \equiv x_i \bmod a_i$. On pose $A_i = \prod_{\substack{j=1 \\ j \neq i}}^{n} a_j$. Alors on a $\operatorname{pgcd}(A_1, \cdots, A_n) = 1$ puisque $a_1, \cdots, a_n$ sont des éléments premiers entre eux deux-à-deux. Ici dit, par l'identité de Bezout, qu'il existe $u_i \in A$ tels que*

$$A_1 u_1 + \cdots + A_n u_n = 1$$

Il vient que

$$A_i u_i \equiv \begin{cases} 0 \bmod a_j, & \text{si } j \neq i \\ 1 \bmod a_i \end{cases}$$

Ceci implique qu'on peut définir x comme

$$x = x_1 A_1 u_1 + \cdots + x_n A_n u_n.$$

En effet, la congruence précédente montre que

$$\forall i = 1, \cdots, n, \ x = x_1 A_1 u_1 + \cdots + x_n A_n u_n \equiv x_i \bmod a_i.$$

5.2 Eléments inversibles mod n

PROPOSITION 5.2.1 *Soit m un entier strictement positif et a un entier relatif. Les conditions suivantes sont équivalentes*

(i) $\overline{a}$ est un générateur du groupe $\mathbb{Z}/m\mathbb{Z}$,

(ii) $\overline{a}$ est inversible dans l'anneau $\mathbb{Z}/m\mathbb{Z}$,

(iii) a est premier à m.

On note $\varphi(m)$ le cardinal de $(\mathbb{Z}/m\mathbb{Z})^\times$. La fonction $\varphi(m)$ est appelée la fonction indicatrice d'Euler. On a la relation suivante :

$$\varphi(m) = m \prod_{p \in \mathcal{P} \,\big|\, p|m} \left(1 - \frac{1}{p}\right) = \prod_{i=1}^{r} p_i^{m_i - 1}(p_i - 1).$$

PREUVE de i) et ii) est déjà fait dans la Proposition 2.3.1 (sur la simplification dans $\mathbb{Z}/n\mathbb{Z}$) : si $\operatorname{pgcd}(a, n) = 1$ et

$$ax \equiv ay \pmod{n}$$

alors $x \equiv y \pmod{n}$.

On va déduire iii) de l'isomorphisme d'anneaux

$$\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/(p_1^{m_1} \cdot \ldots \cdot p_r^{m_r}) \xrightarrow{\sim} \prod_{i=1}^{r} \mathbb{Z}/(p_i^{m_i}).$$

En considérant les éléments inversibles, on obtient un isomorphisme de groupes

$$(\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{\sim} \prod_{i=1}^{r} (\mathbb{Z}/(p_i^{m_i}))^\times.$$

Par conséquant

$$\varphi(m) = \prod_{i=1}^{r} \varphi(p_i^{m_i}).$$

Mais si p est premier, a est premier à p si et seulement s'il n'est pas divisible par p.
Donc

$$\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1),$$
$$\varphi(p_1^{n_1} \cdot \ldots \cdot p_r^{n_r}) = p_1^{n_1-1}(p_1-1) \cdot \ldots \cdot p_r^{n_r-1}(p_r-1).$$

EXEMPLE.

$$\varphi(4) = 2, \varphi(25) = 20, \varphi(100) = 40, \varphi(1000) = 4 \cdot 100 = 400.$$

EXERCICE. Trouver la factorisation en produit des nombres premiers de $\varphi(8!)$.

REMARQUE. Le problème de calcule de $\varphi(n)$ est difficile pour les grands nombres entiers n, puisque il dépend de la factorisation de n.

COROLLAIRE 5.2.2 (THÉORÈME DE FERMAT-EULER) *Pour tout entier strictement positif n et tout élément a de $(\mathbb{Z}/n\mathbb{Z})^\times$, on a*

$$a^{\varphi(n)} = 1.$$

PREUVE. Cela résulte du théorème de Lagrange (théorème 3.6.3), appliqué au groupe $(\mathbb{Z}/n\mathbb{Z})^\times$.

EXEMPLE.

```
> 3&^400 mod 100000;
```

88001

5.3 Application à la cryptographie : RSA

La *cryptographie théorique* est une science qui étudie les systèmes d'échange d'information protégé.

On considère un système d'utilisateurs $U_1, U_2, U_3 \ldots$. De temps en temps chaque couple d'utilisateurs aurait pu besoin d'échanger de messages que doivent rester secret pour les autres utilisateurs ou pour toute autre person non autorisée.

Dans les *systèmes classiques* de cryptographie, ils doivent échanger d'abord les clés et après les garder secret. La cryptographie à *clef publique* évite la dernière restriction : les communications secretes deux-à-deux devienent possible en utilisant seulement une information ouverte pour tout le monde. Un tel système peut être réalisé de façon suivante : Pour l'ensemble $\{U_i\}$ d'utilisateurs et un ensemble fini $\mathcal{M}$ des "messages" , et on associe à tout U_j deux applications

$$\mathcal{E}_j : \mathcal{M} \to \mathcal{M}, \text{ et } \mathcal{D}_j : \mathcal{M} \to \mathcal{M},$$

de telle façon que $\mathcal{D}_j$ est secret, $\mathcal{E}_j$ est publique (ouverte), et

$$\mathcal{E}_j \circ \mathcal{D}_j = id = \mathcal{D}_j \circ \mathcal{E}_j : \mathcal{M} \to \mathcal{M}.$$

(donc le savoir de $\mathcal{E}_j$ ne donne pas $\mathcal{D}_j = \mathcal{E}_j^{-1}$.

Cryptographie asymétrique.

Les méthodes anciennes utilisées pour cryptage et pour décryptage ont été *symétriques* : les applications

$$\mathcal{E}_{ij} : \mathcal{M} \to \mathcal{M}, \text{ et } \mathcal{D}_{ij} : \mathcal{M} \to \mathcal{M},$$

ont été connu pour U_i et U_j, mais secrets pour tout autre utilisateur U_k, avec $k \neq i, j$.

Par exemple, on a utilisé souvent le cryptage *par permutation* $\mathcal{E}_{ij}$, ou cryptage par *addition avec un grand nombre aléatoire* dans $\mathcal{M} = \mathbb{Z}/N\mathbb{Z}$.

En 1976, des nouveaux systèmes de cryptographie *asymétriques* ont été découverts par Diffie, Hellman, Rivest, Shamir, Adleman à la base de la difficulté du *problème d'inversion*.

Fonctions sens unique à trappe.

Soient $\mathcal{E}$ et $\mathcal{F}$ deux ensembles finis, par exemple $\mathcal{E} = \mathcal{F} = \mathcal{M}$. Une fonction ψ bijective de $\mathcal{E}$ dans $\mathcal{F}$ est dite une *fonction sens unique* (FSU) si étant donné $y \in \mathcal{F}$ tel qu'il existe $x \in \mathcal{E}$ avec $\psi(x) = y$, la seule donnée de ψ et de y ne permet pas de calculer x ; c'est le *problème d'inversion*, c'est-à-dire calculer la fonction inverse ψ^{-1} de ψ. La fonction ψ est dite *fonction sens unique à trappe* (FSUT) si c'est une FSU telle que il existe une information supplémentaire, la *clé secrète* $\mathcal{K}$, qui permet de résoudre le problème d'inversion.

Utilisations des fonctions sens unique à trappe.

Soit ψ une FSUT de $\mathcal{E}$ dans $\mathcal{F}$ avec la clé secrète $\mathcal{K}$. Les messages possibles sont les éléments de $\mathcal{E}$ et les messages cryptés sont les éléments de $\mathcal{F}$. Afin de recevoir des messages cryptés, *Alice* (un utilisateur) rend publique la fonction ψ (fonction de cryptage), elle garde secret néanmoins la clé $\mathcal{K}$. Pour transmettre un message $x \in \mathcal{E}$ à *Alice*, *Bob* calcule $y = \psi(x)$ et envoie y. Afin de décoder le message y, il faut pouvoir calculer $x = \psi^{-1}(y)$, or seule *Alice*, qui possède $\mathcal{K}$, arrive à calculer ψ^{-1} (fonction de décryptage). Ainsi, tout le monde peut coder un message, mais seule *Alice* peut le décoder.

5.4 Principaux protocoles.

Les principaux protocoles existants utilisant des FSU ou des FSUT sont le protocole RSA, et les protocoles de type ElGamal basés sur le problème du logarithme discret : dans le groupe des éléments inversibles d'un corps fini ou dans le groupe des points d'une courbe elliptique sur un corps fini.

Le protocole RSA (comme Rivest, Shamir, Adleman), voir [RSA]

Soient p et q deux nombres premiers de grande taille, on pose $n = p \cdot q$. L'ensemble $\mathcal{E}$ et l'ensemble $\mathcal{F}$ sont le même ensemble : l'ensemble $\mathcal{M} = \{0, \ldots, n-1\}$ des nombres entiers entre 0 et $n-1$. Soit e un nombre entier premier avec $(p-1)(q-1)$. La fonction ψ est la fonction

$$\psi(x) = x^e \mod n,$$

la clef secrète $\mathcal{K}$ est un entier d tel que

$$e \cdot d \equiv 1 \pmod{(p-1)(q-1)},$$

alors on a

$$\psi^{-1}(x) = x^d \pmod{n}.$$

Cette assertion est vraie pour tous les $x \mod pq$.

Si $\text{pgcd}(x, pq) = 1$, on utilise le théorème 5.2.2 d'Euler-Fermat :

$$x^{ed} \equiv x \bmod pq.$$

Si, par exemple $p|x$, mais $q \nmid x$, on a donc

$$ed = 1 + (p-1)(q-1)t \Rightarrow x^{ed} = (x)^{1+(p-1)(q-1)t} = x(x^{(p-1)t})^{q-1} \equiv x \bmod pq$$
$$\Rightarrow x^{ed} = \begin{cases} x((x)^{(p-1)})^{q-1} \equiv x \cdot 1 \bmod q, \\ \equiv 0 \equiv x \bmod p \end{cases} \quad \Rightarrow x^{ed} \equiv x \bmod pq.$$

La sécurité du protocole RSA

réside sur le fait que pour calculer l'entier d, il faut connaître les nombres p et q, et donc être à même de factoriser l'entier n.

Pour réaliser ce schéma on utilise la difficulté technique de factorisation de grands nombres entiers en produit de nombres premiers.

Système RSA pour plusieurs utilisateurs

a). Chaque utilisateur U_i choisit deux grand nombres premiers p_i, q_i, et deux classes $e_i, d_i \bmod n_i$ où $n_i = p_i q_i$ telles que $e_i d_i \equiv 1 \bmod \varphi(n_i)$ où $\varphi(n_i) = (p_i - 1)(q_i - 1)$ désignes la fonction de Euler.

b). Les nombres (e_i, n_i) sont publiques pour tous les utilisateurs (ils sont publiés dans une sorte de "pages blanches").

On suppose qu'il n'est pas possible de calculer d_i à partir de (e_i, n_i), donc d_i peut être consideré comme une clef secrète de décryptage connue seulement à U_i. En effet, on montrera qu'un algorithme efficace pour calculer d_i trouve aussi la *factorisation* de n_i (ceci dit, un tel algorithme est *équivalente* à la résolution d'un problème supposé difficile). Supposons qu'on connait d_i. Alors on connait que $\varphi(n_i)$ *divise* $e_i d_i - 1$. Si l'on avait connu $\varphi(n_i)$ on aurait pu trouver facilement p_i, q_i car

$$\varphi(n_i) = (p_i - 1)(q_i - 1) = p_i q_i - (p_i + q_i) + 1 \Rightarrow$$
$$p_i + q_i = n_i + 1 - \varphi(n_i) \text{ et } p_i - q_i = \sqrt{(p_i + q_i)^2 - 4n_i}.$$

On peut montrer même que si l'on connait seulement un multiple de $\varphi(n_i)$ on puisse trouver p_i, q_i.

c). Supposons qu'un utilisateur U_i souhaite à transmettre à U_j un message secret repésenté comme un suite de bits. Tout d'abord, il décompose cette suite en blocs de longueur $[\log_2 n_j]$, alors il considère tout bloc comme une classe des résidue $m \bmod n_j$ et finalement il crypte le message par la classe $m^{e_j} \bmod n_j$. Ceci dit, (n_j, e_j) sers comme une clef de cryptage de j-e utilisateur.

d). Ayant reçu le message crypté, U_j le décrypte bloc-par-bloc $b \bmod n_j$ par calcule de $b^{d_j} \bmod n_j$ (rapellons qu'il connait seulement sa clef de décryptage d_j). Ceci est impliqué immédiatement par le théorème d'Euler-Fermat (corollaire 5.2.2).

Exemple de cryptage avec RSA

On suppose qu'on travaille avec un alphabet de N symboles, alors on utilise une base d'écriture $= N$. Soient $k < l$ deux entiers strictement positifs tel que $N^k < n_j < N^l$, par exemple $k = [\log_N n_j]$. Alors les blocs de k lettres correspondent aux nombres $0 \leq m << n_j$. Tout message est présenté comme une suite de tel blocs, et on crypte par blocs $M = m \bmod n_j$. Soit $f(M) = \mathcal{E}_j(M)$, $f : \mathbb{Z}/n_j\mathbb{Z} \to \mathbb{Z}/n_j\mathbb{Z}$. L'image $f(M)$ peut être présentée comme un bloc de l lettres car $n_j < N^l$ mais pas tous les blocs de l lettres paraissent de telle façon.

Exemple. Soit $N = 26$ (l'alphabet de 26 lettres), $p_j = 281$, $q_j = 167$, $n_j = 46927$, $e_j = 39423$, $d_j = 26767$, $k = 3$, $l = 4$,

$$N^3 = 17576 < 46927 < N^4 = 456976.$$

Le mot "YES" correspond à $24 \cdot N^2 + 4 \cdot N + 18 = 16346 = m \bmod n_j$.

$$16346^{39423} \bmod 46927 = 21166 = 1 \cdot 26^3 + 5 \cdot 26^2 + 8 \cdot 26 + 2 = \text{ "BFIC" } = \bmod n_j$$

Pour décrypter le message, l'utilisateur U_j applique

$$b \mapsto b^{d_j} \bmod n_j,\ 21166^{26767} \bmod 46927 = 16346.$$

Signatures éléctroniques

Bien évidemmement, on peut varier les détails de ce schéma *ad infinitum*. Par exemple, on peut construire une procédure d'authentification ("electronic signature") qui utilise une forme *signé* d'un message secret de U_i à U_j permettant U_j de convaincre une troisième personne (un "juge") que l'auteur du message est bien U_i donc ce message n'été pas falcifié par U_j lui-même. Ceci peut être crucial pour certaines transactions interbancaires.

On considère l'application $\mathcal{E}_i$ de cryptage pour les messages adressés à U_i et soit $\mathcal{D}_i$ l'application de décryptage de U_i. Alors on a vu que $\mathcal{E}_i$ est publique tandis que $\mathcal{D}_i$ est privé (la propriété de U_i). Pour tout message M on a $\mathcal{D}_i(\mathcal{E}_i(M)) = M$ et $\mathcal{E}_i(\mathcal{D}_i(M)) = M$. L'utilisateur U_i en envoiant à U_j son message M utilise comme sa signature $S = \mathcal{D}_i(M)$ et il transmet à U_j sa version cryptée $\mathcal{E}_j(S)$. A son tour, U_j d'abord calcule $S = \mathcal{D}_j(\mathcal{E}_j(S))$ et ensuite $M = \mathcal{E}_i(S)$ en utilisant la clef publique $\mathcal{E}_i$. Le récépteur peut convaincre un juge que M vient de U_i parce que seulement avec l'application $\mathcal{E}_i$ on peut transformer S en un message sensé M.

De plus, le récépteur de $S = \mathcal{D}_i(M)$ ne peut pas le falcifier car il ne connait pas $\mathcal{D}_i$.

Maintenant on discutra plutôt des aspects arithmétiques que les aspects informatiques de la théorie des cryptosystèms à clef publique. On montrera que les résultats classiques de l'arithméique peuvent être appliqués dans ce domaine.

Problème 1. Comment produire des grands nombres premiers ?

On a besoin d'une méthode vraiment efficace pour organiser une production en masse des grands nombres premiers "suffisemment aléatoirs" pour permettre à un utulisateur à calculer (à l'aide d'un ordinateur) son couple customisé (p_i, q_i) et d'être sûr qu'aucun autre utilisateur ne prendra cette paire.

Problème 2. Comment factoriser grands nombres entiers ?

Ce problème est clé pour la troisième partie qui souhaite casser le cryptosystème mais aussi, bien-sûr, pour les développeurs essayant assurer la fiaibilité d'un tel système.

Le protocole ElGamal

Ce protocole s'applique dès que l'on a un groupe cyclique fini G. On fixe g un générateur de G et on note M l'ordre du groupe G. L'ensemble $\mathcal{E}$ est égal à G et l'ensemble $\mathcal{F}$ est une partie du produit $G \times G$, c'est-à-dire à l'ensemble formé des couples de deux élément de G. *Alice* choisit, au hasard, un élément a dans $\{0, \ldots, M-1\}$ et calcule g^a. Puis elle rend publique G, g et g^a. La clé secrète $\mathcal{K}$ est l'entier a. Pour crypter un message $x \in G$, *Bob* choisit un entier k au hasard dans $\{0, \ldots, M-1\}$ et calcule $y_1 = g^k$, puis $y_2 = x \cdot (g^a)^k$ (ce qui est possible puisque g^a est publique). Le message crypté est le couple $(y_1, y_2) \in G \times G$.

La fonction de cryptage FSUT

En d'autres termes, la fonction de cryptage FSUT ψ est donnée par

$$\psi(x) = \left(g^k, x \cdot (g^a)^k\right)$$

avec k un entier choisi au hasard dans $\{0, \ldots, M-1\}$ et différent à chaque fois. Pour décrypter un tel message (y_1, y_2), *Alice* calcule y_1^{-a} et obtient

$$y_1^{-a} \cdot y_2 = g^{-ak} \cdot x \cdot g^{ak} = g^{ak-ak} \cdot x = x.$$

La sécurité du protocole ElGamal

Ainsi la fonction de décryptage

$$\psi^{-1}(y_1, y_2) = y_1^{-a} \cdot y_2$$

n'est calculable que si on connaît la clé secrète $\mathcal{K}$.

La sécurité de ce protocole repose sur la difficulté de résoudre le *problème du logarithme discret*. Plus précisément, le problème de retrouver l'entier a étant donnés g et g^a. C'est un problème difficile dans la plupart des cas si l'ordre du G groupe est divisible par un grand nombre premier.

Exercices

5.1. *On considère l'équation*

$$X^2 - X = 0$$

Trouver toutes ses solutions dans les anneaux

$$\mathbb{Z}/100\mathbb{Z}, \mathbb{Z}/72\mathbb{Z}, \mathbb{Z}/p^n\mathbb{Z}.$$

5.2. *Soit p, q deux nombres premiers. Combien l'équation*

$$X^3 - X = 0$$

a-t-elle de solutions dans les anneaux

$$\mathbb{Z}/pq\mathbb{Z}, \mathbb{Z}/72\mathbb{Z}, \mathbb{Z}/p^n\mathbb{Z}.$$

6 Primalité

On considère maintenant la question suivante : le nombre naturel donné est–il premier où composé ?

Une méthode très ancienne du "crible" d'Eratosthène (3e siècle avant notre ère) donne la liste de tous les nombres premiers $\leq n$. Il fournit aussi le plus petit nombre premier qui divise n et donc est un test de primalité, voir ci-desus *Construction d'une table de nombres premiers*.

Cependant elle n'est pas très efficace car elle utilise plus de n divisions, et dépend exponentiellement de la longuer de l'écriture de n.

La démonstration d'Euclide du fait que l'ensemble des nombres premiers est infini utilise la réduction *ad absurdum*. Une démonstration plus moderne est due à Euler : le produit étendu sur tous les nombres premiers

$$\prod_p \left(1 - \frac{1}{p}\right)^{-1} = \prod_p \left(1 + \frac{1}{p} + \frac{1}{p^2} + \ldots\right) \tag{6.1}$$

devrait être fini si l'on suppose que l'ensemble des nombres premiers est fini. Cependant, la partie droite de (6.2.1) se réduit à une série divergente $\sum_{n=1}^{\infty} n^{-1}$ par le théorème de factorisation unique.

Fibonacci a suggeré (en 1202) un test plus rapide de primalité en remarquant que le plus petit diviseur non–trivial de n est $\leq [\sqrt{n}]$ donc il suffit d'essayer seulement de tels nombres.

Rapellons une propriété importante des nombres premiers.

6.1 $\mathbb{Z}/p\mathbb{Z}$ est un corps

THÉORÈME 6.1.1 *Soit $n \geq 2$ un entier. Alors l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.*

PREUVE. $\Rightarrow$ On raisonne par l'absurde : si n n'était pas premier, on aurait une décomposition $n = ab$ avec $a, b < n$ et strictement positifs. Dans ce cas les classes $\overline{a} = a \bmod n$ et $\overline{b} = b \bmod n$ sont non nuls donc inversibles dans le corps $\mathbb{Z}/n\mathbb{Z}$, ce que contrédit l'égalité $\overline{a}\overline{b} = 0$.

$\Leftarrow$ Si n est premier, et $\overline{a} = a \bmod n$ un élément non-nul, alors n ne divise pas a, donc n et a sont premiers entre eux. Par l'identité de Bezout, il existe $u, v \in \mathbb{Z}$ tels que $au + nv = 1$, donc $\overline{au} = 1$ dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, ceci dit , $\mathbb{Z}/n\mathbb{Z}$ est un corps.

6.2 Petit théorème de Fermat

La contribution essentielle suivante dans le problème de vérification de primalité est liée au petit théorème de Fermat (dix–septième siècle). Ce résultat donne une condition nécessaire de primalité

THÉORÈME 6.2.1 (PETIT THÉORÈME DE FERMAT) *Soit n un nombre premier et a premier à n. Alors*

$$a^{n-1} \equiv 1 \bmod n. \tag{6.2}$$

6.3 Nombres pseudopremiers de Fermat

La condition (6.2) (avec a fixe) est nécessaire mais n'est pas suffisante en général pour que n soit premier. Mais si elle n'est pas satisfaite pour n, alors sûrement n est composé (mais en général on ne connaît aucun de ses diviseurs). On appelle n *pseudopremier par rapport à* a si $\mathrm{PGCD}(a, n) = 1$ et la condition (6.2) est satisfaite.

EXEMPLE 6.3.1 *Soit $p = 323$. Est-ce que p est premier ? On calcule 2^{322} modulo 323. On organise les calcules dans une table :*

i	m	m_i	2^{2^i} *mod 323*
0	*322*	*0*	*2*
1	*161*	*1*	*4*
2	*80*	*0*	*16*
3	*40*	*0*	*256*
4	*20*	*0*	*290*
5	*10*	*0*	*120*
6	*5*	*1*	*188*
7	*2*	*0*	*137*
8	*1*	*1*	*35*

Alors

$$2^{322} \equiv 4 \cdot 188 \cdot 35 \equiv 157 \pmod{323},$$

donc 323 n'est pas premier. En effet, $323 = 17 \cdot 19$.

Les nombres composés $n = 561 = 3 \cdot 11 \cdot 17$,$1105 = 5 \cdot 13 \cdot 17$, $1729 = 7 \cdot 13 \cdot 19$ sont pseudopremiers par rapport à tout a (premier à n). On appelle un tel nombre *nombre de Carmichael*.

En 1994 il a été démontré par Alford, Granville et Pomerance que l'ensemble des nombres de Carmichael est infini (voir [AGP94]). Par exemple, un nombre n sans diviseurs carrés est un nombre de Carmichael si et seulement si pour tout diviseur premier p de n, $p - 1$ divise $n - 1$.

De la condition (6.2) provient un test rapide *probabiliste* de vérification de primalité. Il est basé sur l'observation que les grandes puissances a^m mod n peuvent être calculées assez rapidement.

Fermat lui–même a decouvert ce théorème en étudiant les nombres $F_n = 2^{2^n} + 1$. Il a cru qu'ils étaient tous premiers, mais il n'a pu vérifier cela que pour $n \leq 4$. Plus tard Euler a trouvé une factorisation non triviale de $F_5 = 4294967297 = 641 \cdot 6700417$. Aucun nouvau nombre premier de Fermat n'a été trouvé, et beaucoup de mathématiciens croient qu'il n'y a pas plus de tels nombres premiers.

Voici quelques calculs de la factorisation de F_5, F_6, F_7, F_8, avec le logiciel PARI

```
PARI/GP is free software, covered by the GNU General Public License, and
comes WITHOUT ANY WARRANTY WHATSOEVER.

Type ? for help, \q to quit.
Type ?12 for how to get moral (and possibly technical) support.

   realprecision = 28 significant digits
   seriesprecision = 16 significant terms
   format = g0.28

parisize = 4000000, primelimit = 500000
? factor(2^32+1)
%1 =
[641 1]

[6700417 1]

? factor(2^64+1)
%2 =
[274177 1]

[67280421310721 1]

? factor(2^128+1)
%3 =
[59649589127497217 1]

[5704689200685129054721 1]

? factor(2^256+1)
%4 =
[1238926361552897 1]

[93461639715357977769163558199606896584051237541638188580280321 1]
```

(Le dernier calcul a pris quelques seconds sur mon ordinateur)

Cours N°5. Jeudi le 6 novembre 2003

7 Polynômes

7.1 Anneau de polynômes, division euclidienne

Sur un corps fini, il convient de distinguer les polynômes et les fonctions polynômes. Nous revenons donc sur la définition des polynômes.

DÉFINITION 7.1.1 *Si A un anneau commutatif, l'anneau des polynômes à une variable X sur A est l'anneau $A[X]$ formé des suites $(a_i)_{i\in\mathbb{N}}$ d'élément de A telles que $a_i = 0$ sauf un nombre fini d'entiers i. Cet ensemble est muni de la somme*

$$(a_i)_{i\in\mathbb{N}} + (b_i)_{i\in\mathbb{N}} = (a_i + b_i)_{i\in\mathbb{N}}$$

et du produit

$$(a_i)_{i\in\mathbb{N}} \times (b_i)_{i\in\mathbb{N}} = \left(\sum_{i=j+k} a_j b_k\right)_{i\in\mathbb{N}}$$

On a une application injective $A \to A[X]$ qui envoie a sur $(a, 0, \cdots)$, et on identifie A avec son image. Tout élément de $A[X]$ s'écrit de façon unique $\sum_{i\in\mathbb{N}} a_i X^i$, où on note par X la suite :

$$(0, 1, 0, 0, \cdots).$$

Soit A un anneau. Il est commode de voir un polynôme $f(X)$ à coefficients dans A une expression formelle du type

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$$

qui est donnée par la suite de ces coefficients a_0, a_1, …, $a_n \in A$, $n \in \mathbb{N}$ telle que presque tous a_n (sauf un nombre fini) sont nuls.

Si tous les coefficients a_i sont nul on appelle $f(X)$ polynôme nul : $f = 0$. Si $f(X)$ est non-nul soit $a_n \neq 0$.

DÉFINITION 7.1.2 *Le plus grand indice n avec cette propriété est appele le* degré *de $f(X)$ et il est noté* $\deg f$. *Le degré du polynîme nul n'est pas défini, mais parfois on pose* $\deg 0 = -\infty$.

L'anneau $A[X]$ est défini comme l'ensemble des expressions $f(X)$ ci-dessus avec des opérations données par les règles suivants : si

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0, \quad a_n \neq 0$$
$$g(X) = b_s X^s + b_{s-1} X^{s-1} + \cdots + b_0, \quad b_s \neq 0$$

deux polynômes et si par exemple $n \geq s$, on appelle leur somme le polynôme

$$(f + g)(X) = f(X) + g(X) = c_n X^n + c_{n-1} X^{n-1} + \cdots + c_0,$$

dont les coefficients sont obtenus par l'addition des coefficients correspondents de X dans f et dans g, c'est à dire $c_i = a_i + b_i$, $i = 0, 1, \ldots, n$, où pour $i > s$ les coefficients b_i sont considérés comme zéros.

Le produit des polynômes $f(X)$ et $g(X)$ est le polynôme

$$(fg)(X) = f(X) \cdot g(X) = d_{n+s} X^{n+s} + d_{n+s-1} X^{n+s-1} + \cdots + d_0,$$

où

$$d_i = \sum_{k+l=i} a_k b_l,$$

et les coefficients a_i, b_j sont considérés comme zéros pour $i > n$, et $j > s$, $d_0 = a_0 b_0$, $d_1 = a_0 b_1 + a_1 b_0$, …, $d_{n+s} = a_n b_s$.

THÉORÈME 7.1.3 *Si l'anneau A n'a pas diviseurs de zéro, l'anneau des polynômes $A[X]$ aussi n'a pas de diviseurs de zéro. Le degré du produit des polynômes non nuls est égal à la somme de ces degrés.*

Démonstration est directement entraîné des formules ci-dessus, en particulière de $d_{n+s} = a_n b_s$, où $n = \deg f$, $s = \deg g$.

L'anneau A peut être s'identifié avec un sous-anneau de $A[X]$ formé par des constantes (polynômes de degré nul et le polynôme nul). Ceci implique que la multiplication des élémets $a \in A$ par $f(X) \in A[X]$ est aussi définit. En particulier, si $A = K$ est un corps, l'anneau $K[X]$ est aussi un éspace vectoriel. Du point de vu de la structure algébrique l'anneau $K[X]$ devient un algèbre de dimension infini sur K, c'est à dire, un anneau et un espace vectoriel en même temps dans lequel la multiplication d'éléments commute avec multiplication par des constantes.

7.2 Division euclidienne sur les anneaux

Division des polynômes avec reste

PROPOSITION 7.2.1 *Soit A un anneau commutatif intègre. On se donne un polynôme*

$$P(X) = \sum_{i=0}^{d} a_i X^i$$

à coefficients dans A telle que a_d soit un élément inversible de A. Alors pour tout polynôme $f(X)$ de $A[X]$ il existe une unique paire $(Q, R) \in A[X]^2$ telle que

$$f = PQ + R \text{ avec } R = 0 \text{ ou } \deg R < \deg P$$

PREUVE. Existence. Nous allons procédé par récurrence sur le degré de f. Si $\deg f < d$, alors $(0, f)$ convient. Sinon on écrit

$$f = \sum_{i=0}^{n} b_i X^i \text{ avec } b_n \neq 0 \text{ et } n \geq d.$$

Alors

$$f - b_n a_d^{-1} X^{n-d} P = PQ_1 + R_1 \text{ avec } R_1 = 0 \text{ ou } \deg R_1 < d.$$

La paire $(Q_1 + b_n a_d^{-1} X^{n-d}, R_1)$ convient.

Unicité. Si

$$PQ_0 + R_0 = PQ_1 + R_1$$

avec $\deg R_0 < \deg P$ et $\deg R_1 < \deg P$ alors $P(Q_0 - Q_1) = (R_1 - R_0)$. Comme le coefficient dominant de P est inversible, on a $\deg(P(Q_0 - Q_1)) = \deg P + \deg(Q_0 - Q_1)$ mais ce degré est strictement inférieur à celui de P si et seulement si $Q_0 - Q_1 = 0$, c'est à dire, $Q_0 = Q_1$, ce qui entraîne que $R_0 = R_1$.

EXEMPLE. Illustrons sur un exemple la façon d'effectuer une telle division dans $\mathbb{Z}[X]$:

$$\begin{array}{r|l} 3X^4 + 7X^3 - 7X^2 + 16X - 5 & X^2 + 3X - 2 \\ \cline{2-2} -3X^4 - 9X^3 + 6X^2 & 3X^2 - 2X + 5 \\ \cline{1-1} -2X^3 - X^2 + 16X - 5 & \\ 2X^3 + 6X^2 - 4X & \\ \cline{1-1} 5X^2 + 12X - 5 & \\ -5X^2 - 15X + 10 & \\ \cline{1-1} -3X + 5 & \end{array}$$

Division euclidienne dans $K[x]$ sur un corps K

THÉORÈME 7.2.2 *Pour tous polynômes $f(X)$ et $P(X)$ tels que $P(X)$ soit non nul à coefficients dans un corps K il existe une unique paire $(Q, R) \in A[X]^2$ telle que*

$$f = PQ + R \text{ avec } R = 0 \text{ ou } \deg R < \deg P$$

Les polynômes $Q(X)$ et $R(X)$ sont uniquement déterminés par cette condition.

DÉFINITION 7.2.3 *Le polynôme $Q(X)$ est appellé le* quotient *de la division $f(X)$ par $Q(X)$, et $R(X)$ le* reste.

Divisibilité des polynômes

Soit K un corps. Soient $f(X)$, $\phi(X) \in K[X]$. Si le reste de la division de $f(X)$ par $\phi(X)$ est nul, on dit que $f(X)$ est divisible par $\phi(X)$ où de même que $\phi(X)$ divise $f(X)$, la notation : $\phi \mid f$. La condition $\phi \mid f$ est équivalente au fait qu'il existe un polynôme $\psi(X)$ tel que $f(X) = \phi(X) \cdot \psi(X)$.

La définition implique directement les propriétés suivantes de la divisibilité :

1) Si f est divisible par g, est g est divisible par h, f est divisible par h.

2) Si f et g sont divisibles par ϕ, leur somme et leur différence sont divisibles par ϕ.

3) Tout polynôme est divisible par n'importe quel polynôme de degré zéro.

4) $f(X)$ divise $g(X)$ et $g(X)$ divise $f(X)$ en même temps si et seulement si $g(X) = cf(X)$, où $c \in K^*$ est un élément inversible.

5) Les ensembles de diviseurs de $f(X)$ et $cf(X)$ coïncident.

On appelle le pgcd (le plus grand diviseur commun) de $f(X)$ et $g(X)$ le polynôme $d(X)$ tel que d divise f et g, et d est divisible par tout autre diviseur commun de ces polynômes.

THÉORÈME 7.2.4 *Pour tous polynômes f et g dans $K[X]$ sur un corps K il existe leur pgcd que est uniquement déterminé à constante multiplicative près.*

C'est une propriété générale dans les anneaux euclidiens.

7.3 Valeurs et racines d'un polynôme

PROPOSITION 7.3.1 *Soit A un anneau commutatif. On se donne un polynôme*

$$f(X) = \sum_{i=0}^{n} a_i X^i$$

à coefficients dans A, et soit c un élément de A. Alors la valeur de f en c est définie comme $f(c) = a_n c^n + a_{n-1} c^{n-1} + \cdots + a_0 \in A$.

(a) L'application

$$\psi_c : A[X] \to A, f \longmapsto f(c) = \sum_{i=0}^{n} a_i c^i \in A$$

est un seul morphisme d'anneaux tel que la réstriction de ψ_c sur le sous-anneau $A \subset A[X]$ soit triviale, et que $\psi_c(X) = c$.

(b) Réciproquement, pour tout morphisme d'anneaux $\psi : A[X] \to A$ tel que la réstriction de ψ sur le sous-anneau $A \subset A[X]$ soit triviale, il existe un seul $c \in A$ tel que $\psi = \psi_c$.

PREUVE de la proposition 7.3.1 découle de la définition 4.1.2 de morphisme d'anneaux.

Fonctions polynômes.

DÉFINITION 7.3.2 *(a) L'application*

$$f : A \to A, c \longmapsto f(c)$$

notée par la même lettre f, est dit la fonction polynôme.

(b) Si $f(c) = 0$ (c'est à dire f s'annule en c), on appelle c racine *de f.*

REMARQUE. La fonction polynôme en général ne défini pas le polynôme de manière unique. Par exemple, sur un corps fini K, il convient de distinguer les polynômes et les fonctions polynômes.

Soit par exemple $A = K = \mathbb{F}_2 = \{0, 1\}$ (le corps de deux éléments). Considérons le polynôme $f(X) = X^2 + X + 1$, alors $f(0) = 1$ et $f(1) = 1$ c'est à dire f definie une fonction constante sur K mais $f(X)$ n'est pas une constante (polynôme de degré zéro) comme polynôme.

THÉORÈME 7.3.3 *Soit $A = K$ un corps. Si $f(X) \in K[X]$, le reste de la division de $f(X)$ par $(X - c)$ est égal à $f(c)$. En particulier, c est une racine de $f(X)$ si et seulement si $f(X)$ est divisible par $X - c$.*

Démonstration est impliquée par l'unicité de la division avec reste :

$$f(X) = q(X)(X - c) + r,$$

où $r = f(c)$.

COROLLAIRE 7.3.4 *Si $f(X) \in K[X]$, le nombre des racines $c \in K$ est majoré par le degré* $\deg(f)$.

Démonstration est impliquée par l'unicité de décomposition en facteurs irréductibles dans un anneau euclidien.

Méthode d'Hörner

permet de trouver facilement le quotient $q(X)$ de la division par $X - c$

$$f(X) = q(X)(X - c) + r,$$

et la valeur $r = f(c)$.

On considère le polynôme
$f(X) = \sum_{i=0}^{n} a_i X^i$, et sa valeur en $X = c$; on calcule $f(c)$ de façon suivante : soient

$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$, $a_n \neq 0$ un polynôme, et on cherche un autre polynôme $q(X) = b_{n-1} X^{n-1} + b_{n-2} X^{n-2} + \cdots + b_0$, $b_{n-1} \neq 0$ tel que

$$f(X) = (X - c)q(X) + r,$$

En comparant les coefficients des puissances de X on obtient

$$a_n = b_{n-1},\ a_{n-1} = b_{n-2} - cb_{n-1},\ \cdots,$$

$$a_1 = b_0 - cb_1,\ a_0 = r - cb_0,\ r = f(c).$$

Ceci implique

$$b_{n-1} = a_n,\ b_{n-k} = cb_{n-k+1} + a_{n-k} (k = 2, \cdots, n)$$

Il est commode de faire le tableau suivant (le schéma de Hörner)

	a_n	a_{n-1}	$\cdots$	a_1	a_0
c	$b_{n-1} = a_n$	$b_{n-2} = cb_{n-1} + a_{n-1}$	$\cdots$	$b_0 = cb_1 + a_1$	$f(c) = cb_0 + a_0$

La formule de Taylor

Soit K un corps. On se donne un polynôme

$$f(X) = \sum_{i=0}^{n} a_i X^i$$

à coefficients dans K, et soit c un élément de K. Alors il existe $b_1, \cdots, b_n \in K$ tels que

$$f(X) = f(c) + b_1(X-c) + b_2(X-c)^2 + \cdots + b_n(X-c)^n,$$

avec la propriété

$$k!b_k = f^{(k)}(c), \quad k = 1, \cdots, n, \tag{7.1}$$

où

$$f'(X) = na_nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \cdots + a_1$$

est la dérivée formelle de $f(X)$.

PREUVE. L'existence des $b_1, \cdots, b_n \in K$ découle de la division euclidienne dans $K[X]$, par récurrence à partir de

$$f(X) = (X-c)q(X) + f(c).$$

Ensuite, on deduit la formule (7.1) par récurrence à partir de l'identité :

$$f(X) = f(c) + b_1(X-c) + b_2(X-c)^2 + \cdots + b_n(X-c)^n,$$

en utilisant l'égalité formelle $((X-c)^k)' = k(X-c)^{k-1}$.

7.4 Formule d'interpolation de Lagrange

La formule d'interpolation de Lagrange donne un polynôme sur un corps K de degré inférieure ou égale à n qui prend pour les valeurs distinctes de la variable X en $\alpha_0, \alpha_1, \ldots, \alpha_n \in K$, les valeurs $\beta_0, \beta_1, \ldots, \beta_n \in K$. La solution est donnée par le polynôme de Lagrange

$$f(X) = \sum_{i=0}^{n} \beta_i \frac{(X-\alpha_0)\ldots(X-\alpha_{i-1})(X-\alpha_{i+1})\ldots(X-\alpha_n)}{(\alpha_i-\alpha_0)\ldots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\ldots(\alpha_i-\alpha_n)} \tag{7.2}$$

En effet son degré et inferieure ou égale à n, et $f(\alpha_i) = \beta_i$ $(i = 0, 1, \ldots, n)$.

PROPOSITION 7.4.1 *Le polynome de Lagrange (7.2) est l'unique polynôme*

$$f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0 \in K[X]$$

de degré $\leq n$ tel que $f(\alpha_i) = \beta_i (i = 0, 1, \ldots, n)$ pour arbitraires distincts *éléments α_i $(i = 0, 1, \ldots, n)$ du corps K et pour arbitraires $\beta_i \in K$ $(i = 0, 1, \ldots, n)$.*

En effet si l'on considère les coefficients $a_j (j = 0, 1, \ldots, n)$ comme des inconnues on obtiendrait le système des équations linéaires suivant :

$$\begin{cases} f(\alpha_0) = a_n\alpha_0^n + a_{n-1}\alpha_0^{n-1} + \cdots + a_0 = \beta_0 \\ f(\alpha_1) = a_n\alpha_1^n + a_{n-1}\alpha_1^{n-1} + \cdots + a_0 = \beta_1 \\ \cdots\cdots\cdots\cdots \\ f(\alpha_n) = a_n\alpha_n^n + a_{n-1}\alpha_n^{n-1} + \cdots + a_0 = \beta_n \end{cases}$$

Le déterminant de ce système carrée coïncide (à signe près) avec le déterminant de Vandermonde

$$\begin{vmatrix} 1 & 1 & \ldots & 1 \\ \alpha_0 & \alpha_1 & \ldots & \alpha_n \\ \alpha_0^2 & \alpha_1^2 & \ldots & \alpha_n^2 \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_0^n & \alpha_1^n & \ldots & \alpha_n^n \end{vmatrix} = \prod_{0 \le i < j \le n} (\alpha_j - \alpha_i)$$

qui est non-nul, d'où l'existence et l'unicité des coefficients cherchés $a_j (j = 0, 1, \ldots, n)$ du polynôme $f(X)$ (dans le corps K).

PROPOSITION 7.4.2 *Soit K un corps* infini. *Alors un polynôme $f(X)$ est uniquement déterminé par la fonction polynôme correspondente $c \mapsto f(c) : K \to K$.*

REMARQUE. Au contraire, sur un corps fini K toute fonction $f : K \to K$ est polynômiale, mais le polynôme correspondent f n'est pas uniquement déterminé par cette fonction, car il existe des polynômes non-nuls représentant la fonction identiquement nulle. Par exemple, le polynôme non-nulle de degré p

$$f(X) = X^p - X = \prod_{a \in \mathbb{F}_p} (X - a)$$

s'annule en tous les points du corps $K = \mathbb{Z}/p\mathbb{Z}$.

7.5 Anneau de polynômes à plusieurs variables

DÉFINITION 7.5.1 *Soit A un anneau commutatif. L'anneau des polynômes à n variables peut être défini par récurrence comme*

$$A[X_1, \cdots, X_n] = A[X_1, \cdots, X_{n-1}][X_n].$$

Si $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_n)$ appartient à $\mathbb{N}^n$, on note $X^{\boldsymbol{\alpha}}$ pour le produit $\prod_{i=1}^n X_i^{\alpha_i}$. Tout polynôme s'écrit alors de manière unique

$$P = \sum_{\boldsymbol{\alpha} \in \mathbb{N}^n} a_{\boldsymbol{\alpha}} X^{\boldsymbol{\alpha}}$$

avec $(a_{\boldsymbol{\alpha}})_{\boldsymbol{\alpha} \in \mathbb{N}^n}$ une famille de $A^{\mathbb{N}^n}$ telle que $a_{\boldsymbol{\alpha}} = 0$ sauf pour un nombre fini d'éléments $\boldsymbol{\alpha} \in \mathbb{N}^n$.

Pour un élément $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_n) \in \mathbb{N}^n$, on note $|\boldsymbol{\alpha}| = \sum_{i=1}^n \alpha_i$. On défini alors le degré total d'un polynôme non nul $P = \sum_{\boldsymbol{\alpha} \in \mathbb{N}^n} a_{\boldsymbol{\alpha}} X^{\boldsymbol{\alpha}}$ comme

$$\deg(P) = \sup\{|\boldsymbol{\alpha}| \mid a_{\boldsymbol{\alpha}} \neq 0\}$$

PROPOSITION 7.5.2 *Soit A un anneau commutatif. Pour tous polynômes non nuls*

$$P, Q \in A[X_1, \cdots, X_n],$$

on a

(i) si $P+Q \neq 0$, *alors* $\deg(P+Q) \leq \sup(\deg P, \deg Q)$
avec l'égalité si $\deg P \neq \deg Q$ *;*
(ii) $\deg(PQ) \leq \deg P + \deg Q)$
avec l'égalité si A *est intègre.*

DÉFINITION 7.5.3 *Soit* A *un anneau commutatif. Un polynôme non nul*

$$P \in A[X_1, \cdots, X_n],$$

est dit homogène *de degré* d *si et seulement si*

$$\boldsymbol{\alpha} \in \mathbb{N}^n, |\boldsymbol{\alpha}| \neq d \Rightarrow a_{\boldsymbol{\alpha}} = 0.$$

PROPOSITION 7.5.4 *Soient* A *et* B *deux anneaux commutatifs,* $\phi : A \to B$ *un morphisme d'anneaux, et* $b_1, \ldots b_n$ *des éléments de* B*, il existe un unique morphisme d'anneaux*

$$\psi : A[X_1, \cdots, X_n] \to B, P = \sum_{\boldsymbol{\alpha} \in \mathbb{N}^n} a_{\boldsymbol{\alpha}} X^{\boldsymbol{\alpha}} \longmapsto P(b_1, \ldots b_n) = \sum_{\boldsymbol{\alpha} \in \mathbb{N}^n} a_{\boldsymbol{\alpha}} b_1^{\alpha_1} \cdot \ldots \cdot b_n^{\alpha_n},$$

tel que la réstriction de ψ *sur le sous-anneau* $A \subset A[X_1, \cdots, X_n]$ *coïncide avec* ϕ*.*

EXERCICES

7.1 Soit P un polynôme dans $A[X]$, A anneau commutatif. Montrer que $P(P(X)) - X$ est divisible par $P(X) - X$

7.2 Soit P un polynôme dans $\mathbb{R}[X]$ tel que $P(1) = 1$ et $P(2) = 4$. On pose $B(X) = X^2 - 3X + 2$. Déterminer le reste de la division de P par B.

7.3 Soit P un polynôme dans $\mathbb{Q}[X]$ tel que $P(X) = (X-a)^2(X-b)$ où $a, b \in \mathbb{C}$. En considérant $P'(X)$, montrer que $a, b \in \mathbb{Q}$.

7.4 Soit

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X],$$

et p/q fraction irréductible telle que $P(p/q) = 0$. Montrer que q divise a_n, p divise a_0, et pour tout m, $p - mq$ divise $P(m)$.

7.5 Dans $\mathbb{R}[X]$ montrer qu'il existe un unique polynôme P de degré ≤ 7 tel que $P+1$ soit divisible par $(X-1)^4$, et $P-1$ soit divisible par $(X+1)^4$. Déterminer P

7.6 Soit $a \in \mathbb{Z}$, n un entier ≥ 2 tel que $\text{pgcd}(a, n) = 1$ Montrer que n est premier si et seulement si les polynômes $(X+a)^n$, et $X^n + a$ sont congrus modulo n.

8 Carrés dans $\mathbb{Z}/p\mathbb{Z}$

8.1 Racines primitives

L'idée clé : *Il existe un élément de* $(\mathbb{Z}/p\mathbb{Z})$ *d'ordre* $p-1$.

Polynômes sur $\mathbb{Z}/p\mathbb{Z}$

PROPOSITION 8.1.1 *Soit* $f \in (\mathbb{Z}/p\mathbb{Z})[x]$ *un polynôme non nul sur le corps* $\mathbb{Z}/p\mathbb{Z}$*. Alors il existe au plus* $\deg(f)$ *éléments* $\alpha \in \mathbb{Z}/p\mathbb{Z}$ *tels que* $f(\alpha) = 0$*.*

PREUVE (comparer avec Corollaire 7.3.4). On procède par récurrence sur $\deg(f)$. Les cas $\deg(f) = 0, 1$ sont clairs. On écrit $f = a_n x^n + \cdots + a_1 x + a_0$. Si $f(\alpha) = 0$ alors

$$\begin{aligned} f(x) &= f(x) - f(\alpha) \\ &= a_n(x^n - \alpha^n) + \cdots + a_1(x - \alpha) + a_0(1-1) \\ &= (x-\alpha)(a_n(x^{n-1} + \cdots + \alpha^{n-1}) + \cdots + a_1) \\ &= (x-\alpha)g(x), \end{aligned}$$

pour un polynôme $g(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$. Ensuite, on suppose que $f(\beta) = 0$ avec $\beta \neq \alpha$. Alors $(\beta-\alpha)g(\beta) = 0$, donc, puisque $\beta - \alpha \neq 0$ (et $\text{pgcd}(\beta - \alpha, p) = 1$, on a $g(\beta) = 0$.

Par l'hypothèse de récurrence, g possède au plus $n-1$ racines, donc il y a au plus $n-1$ possibilités pour β. Il vient que f a au plus n racines.

EXEMPLE 8.1.2 *Trouver les racines de*

$$f = x^4 - x^3 + x^2 + x + 1 \in (\mathbb{Z}/3\mathbb{Z})[x].$$

Solution : $f(0) = 1$, $f(1) = 0$, $f(2) = 0$, *donc les racines sont* $\{1, 2\}$. *De plus,*

$$f = (x+1)(x+2)(x^2+2x+2).$$

Bien-sûr, on peut factoriser rapidement ce polynôme mod 3 en Maple :

```
> Factor(x^4 - x^3 + x^2 +x +1)mod 3;
```

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

PROPOSITION 8.1.3 *Soit p un nombre premier, et soit d un diviseur de $p-1$. Alors $f(x) = x^d - 1 \in (\mathbb{Z}/p\mathbb{Z})[x]$ possède exactement d racines.*

PREUVE. Soit e tel que $de = p-1$. On a

$$\begin{aligned} x^{p-1} - 1 &= (x^d)^e - 1 \\ &= (x^d - 1)((x^d)^{e-1} + (x^d)^{e-2} + \cdots + 1) \\ &= (x^d - 1)g(x), \end{aligned}$$

où $\deg(g(x)) = p - 1 - d$. Rapellons que le petit théorème de Fermat implique : $x^{p-1} - 1$ possède exactement $p-1$ racines dans $\mathbb{Z}/p\mathbb{Z}$. Par proposition 8.1.1, $g(x)$ possède *au plus* $p-1-d$ racines et $x^d - 1$ a au plus d racines, donc $g(x)$ possède exactement $p-1$ racines et $x^d - 1$ possède exactement d racines, CQFD.

ATTENTION : L'analogue de ce théorème est faux pour un $f \in (\mathbb{Z}/n\mathbb{Z})[x]$ avec n composé. Par exemple, si $n = n_1 \cdot n_2$ avec $n_1, n_2 \neq 1$, alors $f = n_1 x$ possède au moins *deux* zéros distincts, notamment 0 et $n_2 \neq 0$.

Un autre exemple : $x^2 - 1 \in \mathbb{Z}/8\mathbb{Z}[X]$ posséde 4 racines : $x = \overline{1}, x = \overline{3}, x = \overline{5}, x = \overline{7}$.

La structure de $(\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, \ldots, p-1\}$

Dans cette section on montrera que le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique.

DÉFINITION 8.1.4 *Une* racine primitive *modulo p est un élément de $(\mathbb{Z}/p\mathbb{Z})^*$ d'ordre $p-1$.*

LEMME 8.1.5 *On suppose que $a, b \in (\mathbb{Z}/n\mathbb{Z})^*$ sont d'ordre r et s, respectivement, et que* $\text{pgcd}(r, s) = 1$. *Alors ab est d'ordre rs.*

C'est un fait général sur les éléments d'un groupe, qui *commutent entre eux*.

PREUVE. Lorsque $(ab)^{rs} = a^{rs}b^{rs} = 1$, 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 $\text{pgcd}(s, r_1 r_2) = 1$, il vient que $s = s_1$. Un argument similaire montre que $r = r_1$, donc l'ordre de ab est rs.

THÉORÈME 8.1.6 *Pour tout nombre premier p il existe une racine primitive mod p. Autrement dit, le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique d'ordre $p-1$.*

PREUVE. On écrit

$$p - 1 = q_1^{n_1} q_2^{n_2} \cdots q_r^{n_r}$$

Comme un produit de nombres premiers distincts q_i.

Par la proposition 8.1.3, le polynôme $x^{q_i^{n_i}} - 1$ a exactement $q_i^{n_i}$ racines, et le polynôme $x^{q_i^{n_i-1}} - 1$ a exactement $q_i^{n_i-1}$ racines. Alors il existe un $a_i \in \mathbb{Z}/p\mathbb{Z}$ tel que $a_i^{q_i^{n_i}} = 1$ mais $a_i^{q_i^{n_i-1}} \neq 1$. Un tel a_i est d'ordre $q_i^{n_i}$. Pour tout $i = 1, \ldots, r$, on chosit un tel a_i. Lorsque'on applique le lemme **??** plusieures fois, on voit que

$$a = a_1 a_2 \cdots a_r$$

est d'ordre $q_1^{n_1} \cdots q_r^{n_r} = p - 1$, donc a est une racine primitive.

REMARQUE. Il existe $\varphi(p-1)$ racines primitives modulo p, puisque il y a $q_i^{n_i} - q_i^{n_i-1}$ façons de choisir a_i. Pour le voir, on peut simplement utiliser le fait que le groupe cyclique $(\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$ contient $\varphi(p-1)$ générateurs (voir le proposition 5.2.1). Sinon, on vérifie que deux choix différents de suites $a_1, \ldots, a_r$ définissent deux racines primitives différentes. On suppose que

$$a_1 a_2 \cdots a_r = a_1' a_2' \cdots a_r',$$

avec a_i, a_i' d'ordre $q_i^{n_i}$, pour $i = 1, \ldots, r$. Lorsqu'on élève les deux parties de l'égalité en la puissance $s = q_2^{n_2} \cdots q_r^{n_r}$, on voit que $a_1^s = a_1'^s$. Puisque $\text{pgcd}(s, q_1^{n_1}) = 1$, il existe un t tel que $st \equiv 1 \pmod{q_1^{n_1}}$. Il vient que

$$a_1 = (a_1^s)^t = (a_1'^s)^t = a_1'.$$

Par la simplification de a_1 dans les deux parties, on voit que $a_2 \cdots a_r = a_2' \cdots a_r'$; on répéte cet argument si nécessaire, et on montre que $a_i = a_i'$ pour tout i. Donc les choix différentes de a_i amènent aux choix différents de racines primitives ; autrement dit, si les racines primitives sont les mêmes, alors les a_i coïncident.

Le nombre total des racines primitives est donc égale à

$$(q_1^{n_1} - q_1^{n_1-1}) \cdot \ldots \cdot (q_r^{n_r} - q_r^{n_r-1}) = \varphi(p-1)$$

puisque

$$p - 1 = q_1^{n_1} q_2^{n_2} \cdot \ldots \cdot q_r^{n_r}.$$

Par exemple, il existe $\varphi(16) = 2^4 - 2^3 = 8$ racines primitives mod 17 :

```
> with(numtheory):d:=17;i:=1;for n from 1 to d-1 do
> if (order(n,d)=d-1) then
> printf("i=%d,n=%d mod %d\n"
> ,i,n,d);
> i:=i+1;
> fi;
> od;
```

```
i=1,n=3 mod 17
```

```
i=2,n=5 mod 17

i=3,n=6 mod 17

i=4,n=7 mod 17

i=5,n=10 mod 17

i=6,n=11 mod 17

i=7,n=12 mod 17

i=8,n=14 mod 17
```

EXEMPLE 8.1.7 *Dans cet exemple, on donne une illustration pour la preuve du théorème 8.1.6 dans le cas* $p = 13$. *On a*

$$p - 1 = 12 = 2^2 \cdot 3.$$

Le polynôme $x^4 - 1$ *a les racines* $\{1, 5, 8, 12\}$ *et* $x^2 - 1$ *a les racines* $\{1, 12\}$, *donc on prend* $a_1 = 5$. *Le polynôme* $x^3 - 1$ *a les racines* $\{1, 3, 9\}$, *donc on pose* $a_2 = 3$. *Finalement,* $a = 5 \cdot 3 = 15 \equiv 2 \bmod 13$. *On remarque que les puissances successives de* 2 *sont*

$$2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1,$$

donc 2 *est en réalité d'ordre* 12.

EXEMPLE 8.1.8 *Le résultat est faux si, par exemple* p *est remplacé par une grande puissance de* 2. *Les éléments de* $(\mathbb{Z}/8\mathbb{Z})^*$ *tous sont d'ordre divisant* 2, *mais* $\varphi(8) = 4$.

THÉORÈME 8.1.9 *Soit* p^n *une puissance d'un nombre premier impaire. Alors il existe un élémént de* $(\mathbb{Z}/p^n\mathbb{Z})^*$ *d'ordre* $\varphi(p^n)$, *c'est à dire,* $(\mathbb{Z}/p^n\mathbb{Z})^*$ *est cyclique.*

(en exercice).

Calcul du logarithme discret dans le groupe $(\mathbb{Z}/n\mathbb{Z})^*$

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% %%%%%%%%%%

LOGARITHME DISCRET

```
> restart;with(numtheory);
```

```
Warning, the protected name order has been redefined and unprotected
```

[*GIgcd*, *bigomega*, *cfrac*, *cfracpol*, *cyclotomic*, *divisors*, *factorEQ*, *factorset*, *fermat*, *imagunit*, *index*, *integral_basis*, *invcfrac*, *invphi*, *issqrfree*, *jacobi*, *kronecker*, λ, *legendre*, *mcombine*, *mersenne*, *minkowski*, *mipolys*, *mlog*, *mobius*, *mroot*, *msqrt*, *nearestp*, *nthconver*, *nthdenom*, *nthnumer*, *nthpow*, *order*, *pdexpand*, ϕ, π, *pprimroot*, *primroot*, *quadres*, *rootsunity*, *safeprime*, σ, *sq2factor*, *sum2sqr*, τ, *thue*]

Examples

```
> with(numtheory):
> order(13,100);
```

$$20$$

```
> order(5,8);
```

$$2$$

```
> order(8,12);
```

$$FAIL$$

```
> primroot(20,239);
```

$$21$$

```
> order (%,239);
```

$$238$$

```
> phi (239);
```

$$238$$

```
> dislog:=proc(x::integer,g::integer,p::integer)
> local s, t, n,d;
> s:=g;t:=order(g,p);
> for n from 1 to t do
> if x=s then d:=n;
> fi;
> s:= s*g mod p;  od;
> return (d);
> end proc;
```

$$dislog := \mathbf{proc}(x::integer,\ g::integer,\ p::integer)$$
$$\mathbf{local}\ s,\ t,\ n,\ d;$$
$$s := g\,;$$
$$t := \mathrm{order}(g,\ p)\,;$$
$$\mathbf{for}\ n\ \mathbf{to}\ t\ \mathbf{do}\ \mathbf{if}\ x = s\ \mathbf{then}\ d := n\ \mathbf{end\ if}\,;\ s := s * g \bmod p\ \mathbf{end\ do}\,;$$
$$\mathbf{return}\ d$$
$$\mathbf{end\ proc}$$

```
> dislog(18,5,23);
```

$$12$$

```
> primroot(9048610007);
```

$$5$$

```
> dislog(7320,2,9587);
```

$$389$$

```
> 5^678 mod 9048610007;
```

$$3757843958$$

```
> nextprime(1000);
```

$$1009$$

```
> dislog(15625,5,9048610007);

Warning, computation interrupted
> primroot(1009);
```

$$11$$

```
> 11^345 mod 1009;
```

$$23$$

```
> dislog(23,11,1009);
```

GP/PARI CALCULATOR Version 2.1.1 (released) i686 running cygwin (ix86 kernel) 32-bit version (readline v4.0 enabled, extended help not available)


```
? znprimroot(9048610007)
%1 = Mod(5, 9048610007)
? znlog(15625,%1)
%2 = 6
? znlog(3757843958,%1)
%3 = 678
```

Cours N°6. Jeudi le 13 novembre 2003

Anneau de polynômes à plusieurs variables : exemples

DÉFINITION 7.5.1 Soit A un anneau commutatif. L'anneau des polynômes à n variables peut être défini par récurrence comme

$$A[X_1, \cdots, X_n] = A[X_1, \cdots, X_{n-1}][X_n].$$

Si $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_n)$ appartient à $\mathbb{N}^n$, on note $X^{\boldsymbol{\alpha}}$ pour le produit $\prod_{i=1}^n X_i^{\alpha_i}$. Tout polynôme s'écrit alors de manière unique

$$P = \sum_{\boldsymbol{\alpha} \in \mathbb{N}^n} a_{\boldsymbol{\alpha}} X^{\boldsymbol{\alpha}}$$

avec $(a_{\boldsymbol{\alpha}})_{\boldsymbol{\alpha} \in \mathbb{N}^n}$ une famille de $A^{\mathbb{N}^n}$ telle que $a_{\boldsymbol{\alpha}} = 0$ sauf pour un nombre fini d'éléments $\boldsymbol{\alpha} \in \mathbb{N}^n$.

Pour un élément $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_n) \in \mathbb{N}^n$, on note $|\boldsymbol{\alpha}| = \sum_{i=1}^n \alpha_i$. On défini alors le degré total d'un polynôme non nul $P = \sum_{\boldsymbol{\alpha} \in \mathbb{N}^n} a_{\boldsymbol{\alpha}} X^{\boldsymbol{\alpha}}$ comme

$$\deg(P) = \sup\{|\boldsymbol{\alpha}| \mid a_{\boldsymbol{\alpha}} \neq 0\}$$

```
> restart;
```

EXEMPLE. On considère l'anneau $\mathbb{Z}[X_1, X_2, X_3, X_4]$. On pose

```
> Q:=mul(X[1]-i*X[2]-i*(X[3]+X[4]+1)+1,
> i=0..2) ;
```

$$Q := (X_1 + 1)\,(X_1 - X_2 - X_3 - X_4)\,(X_1 - 2\,X_2 - 2\,X_3 - 2\,X_4 - 1)$$

- Pour développer Q en monômes, on utilise :

```
> expand(Q);
```

$$-2\,X_1\,X_2 - 2\,X_1\,X_3 - 2\,X_1\,X_4 - 3\,{X_1}^2\,X_2 - 3\,{X_1}^2\,X_3 - 3\,{X_1}^2\,X_4 + 2\,X_1\,{X_2}^2 + 2\,X_1\,{X_3}^2 + 2\,X_1\,{X_4}^2 + 2\,{X_2}^2 + 4\,X_2\,X_3 + 4\,X_2\,X_4 + 2\,{X_3}^2 + 4\,X_3\,X_4 + 2\,{X_4}^2 - X_1 + X_2 + X_3 + X_4 + 4\,X_1\,X_2\,X_3 + 4\,X_1\,X_2\,X_4 + 4\,X_1\,X_3\,X_4 + {X_1}^3$$

- Pour développer Q en monômes dans l'ordre lexicographique, on utilise :

```
> sort(expand(Q),[X[1],X[2],X[3],X[4]], plex);
```

$${X_1}^3 - 3\,{X_1}^2\,X_2 - 3\,{X_1}^2\,X_3 - 3\,{X_1}^2\,X_4 + 2\,X_1\,{X_2}^2 + 4\,X_1\,X_2\,X_3 + 4\,X_1\,X_2\,X_4 - 2\,X_1\,X_2 + 2\,X_1\,{X_3}^2 + 4\,X_1\,X_3\,X_4 - 2\,X_1\,X_3 + 2\,X_1\,{X_4}^2 - 2\,X_1\,X_4 - X_1 + 2\,{X_2}^2 + 4\,X_2\,X_3 + 4\,X_2\,X_4 + X_2 + 2\,{X_3}^2 + 4\,X_3\,X_4 + X_3 + 2\,{X_4}^2 + X_4$$

```
>
```

- Pour développer Q suivant les puissances X_1, on utilise :

```
> collect(%,X[1]);
```

$${X_1}^3 + (-3\,X_3 - 3\,X_4 - 3\,X_2)\,{X_1}^2 + (-1 - 2\,X_3 + 2\,{X_4}^2 - 2\,X_4 + 2\,{X_2}^2 + 4\,X_2\,X_3 + 4\,X_2\,X_4 - 2\,X_2 + 2\,{X_3}^2 + 4\,X_3\,X_4)\,X_1 + X_2 + 2\,{X_2}^2 + 4\,X_2\,X_3 + 4\,X_2\,X_4 + 2\,{X_4}^2 + 2\,{X_3}^2 + 4\,X_3\,X_4 + X_3 + X_4$$

- Pour réduire Q modulo 3, on utilise :

```
> Expand(Q) mod 3 ;
```

$$X_1{}^3 + 2\,X_1\,X_2{}^2 + X_1\,X_2\,X_3 + X_1\,X_2\,X_4 + X_1\,X_2 + 2\,X_1\,X_3{}^2 + X_1\,X_3\,X_4 + X_1\,X_3 + 2\,X_1\,X_4{}^2 + X_1\,X_4 + 2\,X_1 + 2\,X_2{}^2 + X_2\,X_3 + X_2\,X_4 + X_2 + 2\,X_3{}^2 + X_3\,X_4 + X_3 + 2\,X_4{}^2 + X_4$$

- Pour développer Q suivant les puissances de X_2 :

```
> collect(expand(Q),X[2]);
```

$$(2\,X_1 + 2)\,X_2{}^2 + (1 + 4\,X_3 + 4\,X_4 - 3\,X_1{}^2 + 4\,X_1\,X_3 + 4\,X_1\,X_4 - 2\,X_1)\,X_2 + X_1{}^3 + 2\,X_3{}^2 - 3\,X_1{}^2\,X_3 - 3\,X_1{}^2\,X_4 + 2\,X_1\,X_3{}^2 + 4\,X_1\,X_3\,X_4 + 4\,X_3\,X_4 + X_3 - 2\,X_1\,X_4 - X_1 - 2\,X_1\,X_3 + 2\,X_1\,X_4{}^2 + 2\,X_4{}^2 + X_4$$

```
>
```

- Pour calculer le degré total de Q, on utilise :

```
> degree(Q,[X[1],X[2],X[3],X[4]]);
```

$$3$$

```
> degree(Q,X[4]);
```

$$2$$

```
> degree(Q,X[1]);
```

$$3$$

```
> degree(Q,[X[1],X[4]]);
```

$$3$$

- Pour trouver le quotient de la division euclidienne de Q par un polynôme de terme dominant inversible (par exemple $X_1^2 + X_1X_2 + X_3$) par rapport à la variable X_1, on utilise :

```
> quo(Q,X[1]^2+X[1]*X[2]+X[3], X[1]);
```

$$X_1 - 3\,X_3 - 3\,X_4 - 4\,X_2$$

- Pour trouver le reste de la division euclidienne de Q par le polynôme de terme dominant inversible $X_1^2 + X_1X_2 + X_3$ par rapport à la variable X_1, on utilise :

```
> rem(Q,X[1]^2+X[1]*X[2]+X[3], X[1]);
```

$$(-1 - 3\,X_3 + 2\,X_4{}^2 - 2\,X_4 + 6\,X_2{}^2 + 7\,X_2\,X_3 + 7\,X_2\,X_4 - 2\,X_2 + 2\,X_3{}^2 + 4\,X_3\,X_4)\,X_1 + X_2 + 2\,X_2{}^2 + 8\,X_2\,X_3 + 4\,X_2\,X_4 + 2\,X_4{}^2 + 5\,X_3{}^2 + 7\,X_3\,X_4 + X_3 + X_4$$

Vérification :

```
> (X[1]^2+X[1]*X[2]+X[3])*(X[1]-3*X[3]-3*X[4]-4*X[2])+(-1-3*X[3]+2*X[4]
> ^2-2*X[4]+6*X[2]^2+7*X[2]*X[3]+7*X[2]*X[4]-2*X[2]+2*X[3]^2+4*X[3]*X[4]
> )*X[1]+X[2]+2*X[2]^2+8*X[2]*X[3]+4*X[2]*X[4]+2*X[4]^2+5*X[3]^2+7*X[3]*
> X[4]+X[3]+X[4];
```

$$(X_1{}^2 + X_1\,X_2 + X_3)\,(X_1 - 3\,X_3 - 3\,X_4 - 4\,X_2) + (-1 - 3\,X_3 + 2\,X_4{}^2 - 2\,X_4 + 6\,X_2{}^2 + 7\,X_2\,X_3 + 7\,X_2\,X_4 - 2\,X_2 + 2\,X_3{}^2 + 4\,X_3\,X_4)\,X_1 + X_2 + 2\,X_2{}^2 + 8\,X_2\,X_3 + 4\,X_2\,X_4 + 2\,X_4{}^2 + 5\,X_3{}^2 + 7\,X_3\,X_4 + X_3 + X_4$$

```
> %-Q;
```

$$(X_1{}^2 + X_1\,X_2 + X_3)\,(X_1 - 3\,X_3 - 3\,X_4 - 4\,X_2) +$$
$$(-1 - 3\,X_3 + 2\,X_4{}^2 - 2\,X_4 + 6\,X_2{}^2 + 7\,X_2\,X_3 + 7\,X_2\,X_4 - 2\,X_2 + 2\,X_3{}^2 + 4\,X_3\,X_4)\,X_1$$
$$+ X_2 + 2\,X_2{}^2 + 8\,X_2\,X_3 + 4\,X_2\,X_4 + 2\,X_4{}^2 + 5\,X_3{}^2 + 7\,X_3\,X_4 + X_3 + X_4$$
$$- (X_1 + 1)\,(X_1 - X_2 - X_3 - X_4)\,(X_1 - 2\,X_2 - 2\,X_3 - 2\,X_4 - 1)$$

```
> expand(%);
```

$$0$$

8.2 Symbole de Legendre.

Soit p, q des nombres premiers impairs distincts. La partie principale de la *loi de réciprocité quadratique* démontrée par Gauss dit que pour $p \equiv q \equiv 3 \bmod 4$ la résolubilité d'une des congruences $x^2 \equiv p \bmod q$ et $x^2 \equiv q \bmod p$ implique la non–résolubilité de l'autre ; sinon elles sont simultanement résolubles ou non–résolubles. Gauss a utilisé ce fait pour des calculs des grandes tableaux de nombres premiers.

Pour cela il a suggéré une modification plus fine de la condition nécessaire de primalité basée sur la congruence de Fermat (6.2). Notamment on définit le symbole de Legendre $\left(\frac{a}{n}\right)$ pour un nombre premier $n = p$ par

$$\left(\frac{a}{n}\right) = \begin{cases} 0 & \text{si } a \equiv 0 \bmod n, \\ 1 & \text{si } a \equiv b^2 \bmod n, \text{ pour un certain } b, n \nmid b, \\ -1 & \text{sinon.} \end{cases} \tag{8.1}$$

PROPOSITION 8.2.1 *Soit $n = p$ un nombre premier impair. L'application*

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

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

Examples

```
> with(numtheory):

Warning, the protected name order has been redefined and
unprotected
```

```
> legendre(74,101);
```

$$-1$$

```
> legendre(3,73);
```

$$1$$

```
> legendre(22,11);
```

$$0$$

```
> legendre(5,2);
```

$$-1$$

```
> legendre(-2342, 1901);
```

$$1$$

8.3 Congruence d'Euler

PROPOSITION 8.3.1 *Soit n un nombre premier impair. Alors*

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \bmod n. \tag{8.2}$$

PREUVE est impliqué par la cyclicité du groupe $(\mathbb{Z}/n\mathbb{Z})^*$. En effet, les deux parties de l'égalité (8.2) sont les morphismes non-triviales du groupe cyclique $(\mathbb{Z}/n\mathbb{Z})^*$ dans le groupe $\{\pm 1\}$. Si n n'est pas nécessairement premier, la congruence (8.2) peut être utilisée comme un test de primalité (une condition nécessaire et suffisante) si l'on définit le symbole de Jacobi à droite par multiplicativité : pour un nombre impair positif $n = p_1 p_2 \dots p_k$, où p_i sont premiers (non nécessairement differents) posons

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_k}\right) \tag{8.3}$$

Cependant, on montrera que le symbole de Jacobi peut être calculé sans connaissance de la factorisation de n en produit des nombres premiers.

REMARQUE. Si n est composé, il se peut que $\left(\frac{a}{n}\right) = 1$ mais a n'est pas un carré $\bmod n$. Par exemple, si $n = pq$, il suffit d'utiliser le théorème chinois des restes pour construire un $a \bmod pq$ tel que $\left(\frac{a}{p}\right) = -1$ et $\left(\frac{a}{q}\right) = -1$. Alors $\left(\frac{a}{n}\right) = 1$ mais a n'est pas un carré $\bmod n$. Au contraire, si a est pas un carré $\bmod n$, alors $\left(\frac{a}{n}\right) = 1$ par multiplicativité.

En effet, le symbole de Jacobi peut être étendu sur toutes les valeurs du "numérateur" et du "dénominateur" et il peut être calculé sans connaissance de la factorisation de n en produit de nombres premiers.

Pour cela on utilise la loi de réciprocité quadratique étendue

$$\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right) = (-1)^{\frac{(P-1)}{2}\frac{(Q-1)}{2}} \tag{8.4}$$

pour P, Q positifs impairs, et on a les deux compléments suivants de cette loi

$$\left(\frac{2}{P}\right) = (-1)^{(P^2-1)/8}, \qquad \left(\frac{-1}{P}\right) = (-1)^{(P-1)/2}, \tag{8.5}$$

aussi bien que la multiplicativité du symbole par rapport au "numérateur" et au "dénominateur". Le calcul suit la même procedure que celle suivie pour l'algorithme d'Euclide et il utilise moins de $5 \log \max(P, Q)$ divisions avec reste.

8.4 Lois de réciprocité de Gauss

(voir [Stein]). Le symbol $\left(\frac{a}{p}\right)$ ne dépends que de la classe résiduelle de a modulo p. Ensuite, on fixe a et on commence par faire une table suivante :

p	$\left(\frac{5}{p}\right)$	$p \bmod 5$
7	-1	2
11	1	1
13	-1	3
17	-1	2
19	1	4
23	-1	3
29	1	4
31	1	1
37	-1	2
41	1	1
43	-1	3
47	-1	2

Cette table fait deviner que $\left(\frac{5}{p}\right)$ ne dépends que de la classe de p modulo 5 ; plus précisemment, $\left(\frac{5}{p}\right) = 1$ si et seulement si $p \equiv 1, 4 \pmod 5$, i.e., p est un carré modulo 5. Cependant, on ne peut pas voir directement de la valeur

$$5^{(p-1)/2} \pmod p,$$

que $p \equiv 1, 4 \pmod 5$ permet d'évaluer cette expression.

A la base de tels calculs, plusieurs mathématiciens ont trouvé une explication conjecturale de ce mystère de 18 siècle. Finalement, Gauss a prouvé cette conjecture en 1801.

THÉORÈME 8.4.1 (LA LOI DE RÉCIPROCITÉ QUADRATIQUE) *Soit p, q des nombres premiers impairs distincts. Alors*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{q}{p}\right), \tag{8.6}$$

c'est à dire que pour $p \equiv q \equiv 3 \bmod 4$ la résolubilité d'une des congruences $x^2 \equiv p \bmod q$ et $x^2 \equiv q \bmod p$ implique la non–résolubilité de l'autre ; sinon elles sont simultanement résolubles ou non–résolubles.

On donnera une démonstration très élémentaire de ce résultat, basé sur le critère de Euler (8.2).

REMARQUE 8.4.2 *Dans l'exemple considéré plus haut, on obtient*

$$\left(\frac{5}{p}\right) = (-1)^{2\cdot\frac{p-1}{2}} \left(\frac{p}{5}\right) = \left(\frac{p}{5}\right) = \begin{cases} +1 & \text{if } p \equiv 1, 4 \pmod 5 \\ -1 & \text{if } p \equiv 2, 3 \pmod 5. \end{cases}$$

Ceci dit, la loi de réciprocité quadratique "explique" pourqoi la connaissance de p modulo 5 permet de calculer $5^{\frac{p-1}{2}} \pmod p$.

Il existe environ 200 démonstration du théorème 8.4.1, voir

`http://www.rzuser.uni-heidelberg.de/~hb3/rchrono.html`

THÉORÈME 8.4.3 (LA LOI DE RÉCIPROCITÉ QUADRATIQUE ÉTENDUE)

$$\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right) = (-1)^{\frac{(P-1)}{2}\frac{(Q-1)}{2}} \tag{8.7}$$

pour P, Q positifs impairs, et on a les deux compléments suivants de cette loi

$$\left(\frac{-1}{P}\right) = (-1)^{(P-1)/2} = \varepsilon(P), \qquad \left(\frac{2}{P}\right) = (-1)^{(P^2-1)/8} = \omega(P), \tag{8.8}$$

où on utilise les fonctions multiplicatives $\varepsilon : (\mathbb{Z}/4\mathbb{Z})^* \to \{\pm 1\}$ *et* $\omega : (\mathbb{Z}/8\mathbb{Z})^* \to \{\pm 1\}$*, données par :*

$$\varepsilon(a) = (-1)^{\frac{a-1}{2}}, = \begin{cases} 1, & si\ a \equiv 1 \pmod 4 \\ -1, & si\ a \equiv 3 \pmod 4 \end{cases}, \quad et\ \omega(a) = (-1)^{\frac{a^2-1}{8}} = \begin{cases} 1, & si\ a \equiv \pm 1 \pmod 8 \\ -1, & si\ a \equiv \pm 3 \pmod 8 \end{cases}.$$

PREUVE découle du théorème 8.4.1 et des définitions (8.20) : si, par exemple, $P = p_1 \cdot \ldots \cdot p_k$, $Q = q_1 \cdot \ldots \cdot q_l$, alors

$$\left(\frac{Q}{P}\right) = \left(\frac{q_1 \cdot \ldots \cdot q_l}{p_1 \cdot \ldots \cdot p_k}\right) = \left(\frac{Q}{p_1}\right) \ldots \left(\frac{Q}{p_k}\right) = \prod_{i=1}^{k} \prod_{j=1}^{l} \left(\frac{q_j}{p_i}\right),$$

$$\left(\frac{P}{Q}\right) = \left(\frac{p_1 \cdot \ldots \cdot p_k}{q_1 \cdot \ldots \cdot q_l}\right) = \prod_{i=1}^{k} \prod_{j=1}^{l} \left(\frac{p_i}{q_j}\right),$$

donc on obtient par multiplicativité :

$$\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right) = \prod_{i=1}^{k} \prod_{j=1}^{l} \left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = \prod_{i=1}^{k} \prod_{j=1}^{l} (-1)^{\frac{p_i-1}{2} \cdot \frac{q_j-1}{2}} = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}},$$

puisque la fonction

$$a \mapsto \varepsilon(a) = (-1)^{\frac{a-1}{2}}, \quad (\mathbb{Z}/4\mathbb{Z})^* \to \{\pm 1\}$$

est multiplicative $\varepsilon(ab) = \varepsilon(a)\varepsilon(b)$. Ensuite, le calcul du symbole de Jacobi suit alors la même procedure que celle suivie pour l'algorithme d'Euclide puisque $\left(\frac{P}{Q}\right)$ ne dépend que de P modulo Q, et il utilise moins de $5 \log \max(P, Q)$ divisions avec reste.

8.5 Une démonstration élémentaire de la loi de réciprocité

Un lemme de Gauss

La preuve donnée dans cette section est basée sur le lemme de Gauss suivant :

LEMME 8.5.1 *Soit p un nombre primier impair, et soit a un entier $\not\equiv 0 \pmod p$. On considère les nombres,*

$$a,\ 2a,\ 3a,\ \ldots,\ \frac{p-1}{2}a$$

et on les reduit modulo p de telle façon que le résultat se trouve dans le ségment $(-\frac{p}{2},\ \frac{p}{2})$. Soit ν le nombre total de nombres négatifs obtenus de cette manière. Alors

$$\left(\frac{a}{p}\right) = (-1)^{\nu}.$$

PREUVE. Pour définir ν, on exprime tout nombre

$$S = \left\{a, 2a, \ldots, \frac{p-1}{2}a\right\}$$

comme un nombre congru au nombre de l'ensemble

$$\left\{1, -1, 2, -2, \ldots, \frac{p-1}{2}, -\frac{p-1}{2}\right\}.$$

Chaque nombre $1, 2, \ldots \frac{p-1}{2}$ apparaît une seule fois, avec un des deux choix de signe, sinon on obtiendrait deux éléments de S qui sont congrus modulo p, ou deux éléments de S dont la somme soit congru à 0 modulo p, ce que est impossible. Alors l'ensemble obtenu doit être de la forme

$$T = \left\{ \varepsilon_1 \cdot 1, \varepsilon_2 \cdot 2, \ldots, \varepsilon_{(p-1)/2} \cdot \frac{p-1}{2} \right\},$$

ou tout ε_i est $+1$ ou-1. En multipliant les éléments de S et de T, on voit que

$$(1a) \cdot (2a) \cdot (3a) \cdot \cdots \cdot \left(\frac{p-1}{2} a \right) \equiv (\varepsilon_1 \cdot 1) \cdot (\varepsilon_2 \cdot 2) \cdots \left(\varepsilon_{(p-1)/2} \cdot \frac{p-1}{2} \right) \pmod{p},$$

donc

$$a^{(p-1)/2} \equiv \varepsilon_1 \cdot \varepsilon_2 \cdot \cdots \cdot \varepsilon_{(p-1)/2} \pmod{p}.$$

Le lemme donc découle de proposition 8.3.1.

Conjecture d'Euler

Tout d'abord, on fait une observation élémentaire :

LEMME 8.5.2 *Soit $a, b \in \mathbb{Q}$. Alors pour tout $n \in \mathbb{Z}$,*

$$\#\left((a,b) \cap \mathbb{Z}\right) \equiv \#\left((a, b+2n) \cap \mathbb{Z}\right) \equiv \#\left((a+2n, b) \cap \mathbb{Z}\right) \pmod{2}.$$

PREUVE. Si $n > 0$, alors

$$(a, b+2n) = (a,b) \cup [b, b+2n),$$

où l'union est disjointe. Soit $[x]$ note la partie entière de x, $[x] \leq x$. Il y a exactement $2n$ entiers dans l'interval $[b, b+2n)$:

$$\begin{cases} b, b+1, \cdots, b+2n-1, & \text{si } b \in \mathbb{Z} \\ [b]+1, [b]+2, \cdots, [b]+2n, & \text{si } b \notin \mathbb{Z} \end{cases}$$

donc l'assertion du lemme est vraie dans ce cas. On a aussi

$$(a, b-2n) = (a,b) \backslash [b-2n, b)$$

et $[b-2n, b)$ aussi contient exactement $2n$ entiers, donc le lemme est vrai aussi pour n négatif. L'affirmation sur $\#\left((a+2n, b) \cap \mathbb{Z}\right)$ est déduit de manière similaire.

La proposition suivante a été conjecturé par Euler, à la base des nombreux calculs. La loi de réciprocité quadratique sera facilement déduit de cette proposition.

PROPOSITION 8.5.3 (CONJECTURE D'EULER) *Soit p un nombre premier impair et $a \in \mathbb{N}$ un nombre entier positif tel que $p \nmid a$.*

1. *Le symbol $\left(\frac{a}{p}\right)$ ne dépend que de p modulo $4a$.*
2. *Si q est un nombre premier tel que $q \equiv -p \pmod{4a}$, alors $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.*

PREUVE.

Pour pouvoir appliquer le lemme de Gauss ci-dessus, on a besoin de calculer la parité du cardinal $\#(S \cap I)$ de l'intersection des ensembles

$$S = \left\{ a, 2a, 3a, \ldots \frac{p-1}{2} a \right\}$$

et

$$I = \left(\frac{1}{2}p, p\right) \cup \left(\frac{3}{2}p, 2p\right) \cup \cdots \cup \left(\left(b - \frac{1}{2}\right)p, bp\right),$$

où soit $b = \frac{1}{2}a$ soit $\frac{1}{2}(a-1)$, on choisit un entier parmi les deux nombres rationnels. En effet, on vérifie que tout élément de S qui se réduit à un nombre dans l' interval $(-\frac{p}{2}, 0)$, appartient à I. Ceci est clair si $b = \frac{1}{2}a < \frac{p-1}{2}a$. Si $b = \frac{1}{2}(a-1)$, alors $bp + \frac{p}{2} > \frac{p-1}{2}a$, donc $((b - \frac{1}{2})p, bp)$ est le dernier intervale qui peut contenir un tel élément de S qui se réduit à $(-\frac{p}{2}, 0)$.) Remarquer aussi que les extrémités entières de I n'appartiennent pas à S, puisque ces extrémités entières sont divisibles par p, mais aucun élément de S est divisible par p.

En divisant I par a, on voit que

$$\#(S \cap I) = \#\left(\mathbb{Z} \cap \frac{1}{a}I\right),$$

où

$$\frac{1}{a}I = \left(\left(\frac{p}{2a}, \frac{p}{a}\right) \cup \left(\frac{3p}{2a}, \frac{2p}{a}\right) \cup \cdots \cup \left(\frac{(2b-1)p}{2a}, \frac{bp}{a}\right)\right).$$

On pose $p = 4ac + r$, et soit

$$J = \left(\left(\frac{r}{2a}, \frac{r}{a}\right) \cup \left(\frac{3r}{2a}, \frac{2r}{a}\right) \cup \cdots \cup \left(\frac{(2b-1)r}{2a}, \frac{br}{a}\right)\right).$$

On observe que la seule différence entre I et J est que les extrémités des intervals sont changés par l'addition d'un entier pair. En appliquant le lemme 8.5.2, on a

$$\nu = \#\left(\mathbb{Z} \cap \frac{1}{a}I\right) \equiv \#(\mathbb{Z} \cap J) \pmod 2.$$

Alors $\left(\frac{a}{p}\right) = (-1)^\nu$ ne dépend que de r, i.e., ne dépend que de p modulo $4a$.

Si $q \equiv -p \pmod{4a}$, alors le seul changement dans le calcul ci-dessus est que r est remplacé par $4a - r$. Ceci remplace l'ensemble $\frac{1}{a}I$ pour l'ensemble

$$K = \left(\left(2 - \frac{r}{2a}, 4 - \frac{r}{a}\right) \cup \left(6 - \frac{3r}{2a}, 8 - \frac{2r}{a}\right) \cup \cdots \cup \left(4b - 2 - \frac{(2b-1)r}{2a}, 4b - \frac{br}{a}\right)\right).$$

Alors K est le même que $-\frac{1}{a}I$, à l'exception de l'addition des entiers pairs aux extrémités. De nouveau, le lemma 8.5.2 implique

$$\#(K \cap \mathbb{Z}) \equiv \#\left(\left(\frac{1}{a}I\right) \cap \mathbb{Z}\right) \pmod 2,$$

donc $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$, CQFD.

L'analyse suivante plus fine dans le cas spécial où $a = 2$ donne aussi une illustration de la démonstration précédente du lemme, et ce résultat est souvent utilisé dans les calculs.

PROPOSITION 8.5.4 *Soit p un nombre premier impair. Alors*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{si } p \equiv \pm 1 \pmod 8 \\ -1 & \text{si } p \equiv \pm 3 \pmod 8 \end{cases}. \tag{8.9}$$

Remarque. La fonction

$$a \mapsto \omega(a) = (-1)^{\frac{a^2-1}{8}} = \begin{cases} 1 & \text{si } a \equiv \pm 1 \pmod 8 \\ -1 & \text{si } a \equiv \pm 3 \pmod 8 \end{cases}, \ \omega : (\mathbb{Z}/8\mathbb{Z})^* \to \{\pm 1\} \tag{8.10}$$

est multiplicative $\omega(ab) = \omega(a)\omega(b)$.
Preuve. Si $a = 2$, l'ensemble $S = \{a, 2a, \ldots, 2 \cdot \frac{p-1}{2}\}$ est

$$\{2, 4, 6, \ldots, p-1\}.$$

Nous pouvons compter la parité des nombres d'éléments de S qui appartiennent à l'interval $I = (\frac{p}{2}, p)$. On pose $p = 8c + r$, alors

$$\begin{aligned} \#(I \cap S) &= \#\left(\frac{1}{2}I \cap \mathbb{Z}\right) = \#\left(\left(\frac{p}{4}, \frac{p}{2}\right) \cap \mathbb{Z}\right) \\ &= \#\left(\left(2c + \frac{r}{4}, 4c + \frac{r}{2}\right) \cap \mathbb{Z}\right) \equiv \#\left(\left(\frac{r}{4}, \frac{r}{2}\right) \cap \mathbb{Z}\right) \pmod 2, \end{aligned}$$

où l'égalité dernière vient du Lemme 8.5.2. Les possibilitiés pour r sont $1, 3, 5, 7$. Si $r = 1$, le cardinal est 0, si $r = 3, 5$ il est 1, et si $r = 7$ il est 2.

Fin de la démonstration de la loi de réciprocité quadratique

Avec le lemme on déduit directement la loi de réciprocité quadratique (théorème 8.4.1 de Gauss) : Soit p, q des nombres premiers impairs distincts. Alors

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

Preuve. On suppose d'abord que $p \equiv q \pmod 4$. Quite à échanger p et q on peut supposer $p > q$, et on pose $p - q = 4a$. Puisque $p = 4a + q$,

$$\left(\frac{p}{q}\right) = \left(\frac{4a+q}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right),$$

on a

$$\left(\frac{q}{p}\right) = \left(\frac{p-4a}{p}\right) = \left(\frac{-4a}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{a}{p}\right).$$

Proposition 8.5.3 implique que $\left(\frac{a}{q}\right) = \left(\frac{a}{p}\right)$, puisque $p \equiv q \pmod{4a}$. Alors

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

où la dernière égalité vient du fait que dans ce cas $\frac{p-1}{2}$ est pair si et seulement si $\frac{q-1}{2}$ est pair.

Ensuite, on suppose que $p \not\equiv q \pmod 4$, alors $p \equiv -q \pmod 4$. On écrit $p + q = 4a$. On a

$$\left(\frac{p}{q}\right) = \left(\frac{4a-q}{q}\right) = \left(\frac{a}{q}\right), \quad \text{and} \quad \left(\frac{q}{p}\right) = \left(\frac{4a-p}{p}\right) = \left(\frac{a}{p}\right).$$

Puisque $p \equiv -q \pmod{4a}$, Proposition 8.5.3 implique que $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$. Mais dans ce cas $(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = 1$, d'où la preuve.

Exemple

EXEMPLE 8.5.5 *Est-ce que* 6 *est un carré modulo* 389 *? On a*

$$\left(\frac{6}{389}\right) = \left(\frac{2\cdot 3}{389}\right) = \left(\frac{2}{389}\right)\cdot\left(\frac{3}{389}\right) = (-1)\cdot(-1) = 1.$$

Ici on a trouvé que $\left(\frac{2}{389}\right) = -1$ *en utilisant Proposition 8.5.4 et le fait que* $389 \equiv 5 \pmod 8$. *On a trouvé* $\left(\frac{3}{389}\right)$ *de manière suivante :*

$$\left(\frac{3}{389}\right) = \left(\frac{389}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Alors 6 *est un carré modulo* 389.

Cependant, on connait pas de x *tel que* $x^2 \equiv 6 \pmod{389}$, *mais on peut le trouver*

```
> restart;for a from 1 to 388 do
> if  a^2 mod 389 = 6 then
> print(a); fi; od;
```

28
361

8.6 Une démonstration de la loi de réciprocité utilisant sommes de Gauss

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

$$\Gamma(s) = \int_0^\infty e^{-y} y^s \frac{dy}{y}. \tag{8.11}$$

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 $(a, N) = 1$ et par $\chi(a) = 0$ pour $(a, N) > 1$. La somme de Gauss $G(\chi)$ est définie par

$$G(\chi) = \sum_{x=1}^{N-1} \chi(x)\zeta_N^x. \tag{8.12}$$

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 (8.11) et (8.12) implique que leurs propriétés sont similaires. Pour les décrire on introduit tout d'abord la notion importante de caractère de Dirichlet primitif. Un caractère χ est dit primitif modulo N s'il ne s'est pas réduit à un autre caractère $\chi' : \mathbb{Z}/M\mathbb{Z} \to \mathbb{C}^*$ définie 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 tout sous–groupe $H_M = ((1+M\mathbb{Z})/(1+N\mathbb{Z}))^\times$ ne soit pas triviale. Par exemple, tout caractère non-triviale modulo un nombre premier q, est primitif, y compris le symbole de Legendre $a \longmapsto \left(\frac{a}{q}\right)$.

PROPOSITION 8.6.1 *Si χ est primitif, on a*

$$G_a(\chi) = \overline{\chi}(a)G(\chi) \ (a \in \mathbb{Z}), \tag{8.13}$$

$$\overline{G(\chi)} = \chi(-1)G(\overline{\chi}), \tag{8.14}$$

$$|G(\chi)|^2 = N. \tag{8.15}$$

REMARQUE 8.6.2 *La propriété (8.13) correspond à la formule*

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

et (8.15), 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 (8.13)–(8.15) (en exercice) est impliquée par des changement d'indice de sommation et par le fait 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 propre diviseur M de N.

Les propriétés (8.13)–(8.15) impliquent la loi de réciprocité quadratique.

Démontrons la formule principale (8.6) :

$$\left(\frac{l}{q}\right)\left(\frac{q}{l}\right) = (-1)^{\frac{l-1}{2}\cdot\frac{q-1}{2}}, \tag{8.16}$$

où l, q sont des nombres premiers distincts. Remarquons premièrement que le symbole quadratique $\chi(a) = \left(\frac{a}{q}\right)$ est un caractère de Dirichlet primitif modulo q. La somme de Gauss correspondante $G(\chi)$ est un élément de l'anneau $R = \mathbb{Z}[\zeta_q]$. Dans un anneau commutatif on a toujours la congruence $(a+b)^l \equiv a^l + b^l \bmod lR$ grâce à la divisibilité des coefficients binomiaux C_l^i par l pour $1 \le i \le l-1$. Comme $\chi^l(a) = \chi(a) = \pm 1$, on a

$$G(\chi)^l \equiv G_l(\chi^l) \bmod lR, \quad G_l(\chi^l) = \overline{\chi(l)}G(\chi),$$

donc

$$G(\chi)^{l-1} \equiv \left(\frac{l}{q}\right) \bmod lR. \tag{8.17}$$

De l'autre côté, $\chi = \overline{\chi}$, et 8.15 implique

$$G(\chi)^2 = \chi(-1)q = (-1)^{\frac{q-1}{2}}q. \tag{8.18}$$

Si l'on représente la partie gauche de (8.17) comme $G(\chi)^2{}^{\frac{l-1}{2}}$ on obtient

$$(-1)^{\frac{q-1}{2}\cdot\frac{l-1}{2}}q^{\frac{l-1}{2}} \equiv \left(\frac{l}{q}\right) \bmod lR. \tag{8.19}$$

Finalement, (8.19) et la congruence d'Euler assurent

$$q^{\frac{l-1}{2}} \equiv \left(\frac{q}{l}\right) \bmod l$$

d'où (8.6).

De façon plus facile on montre l'égalité (8.9) à l'aide de l'anneau $S = \mathbb{Z}[\varepsilon]$, où $\varepsilon = \exp(2\pi i/8)$. On pose $b = \varepsilon + \varepsilon^{-1}$, et on observe que $b^2 = (\varepsilon + \varepsilon^{-1})^2 = 2$. Ensuite $(\varepsilon + \varepsilon^{-1})^p \equiv \varepsilon + \varepsilon^{-1} \bmod pS$ si $p \equiv \pm 1 \bmod 8$, et $(\varepsilon + \varepsilon^{-1})^p \equiv -(\varepsilon + \varepsilon^{-1}) \bmod pS$ si $p \equiv \pm 3 \bmod 8$. De plus, $\bar{b}^2 \equiv 2 \bmod pS$ implique que $\bar{b} = b \bmod pS$ est inversible dans l'anneau quotient

$$S/pS = \langle \varepsilon^n \bmod pS \rangle_{n=0,\cdots,3} = \left\langle 1, \varepsilon, \varepsilon^2, \varepsilon^3 \right\rangle, \quad \varepsilon^4 = -1, \varepsilon^5 = -\varepsilon, \varepsilon^6 = -\varepsilon^2, \varepsilon^7 = -\varepsilon^3,$$

donc $(\varepsilon + \varepsilon^{-1})^p \equiv \varepsilon + \varepsilon^{-1} \bmod pS$ implique $b^p \equiv b \bmod pS$, d'où $b^{p-1} \equiv 1 \bmod pS$, et

$$b^2 \equiv 2 \bmod p \Rightarrow 2^{(p-1)/2} \equiv (b^2)^{(p-1)/2} \equiv b^{p-1} \equiv 1 \bmod pS \Rightarrow 2^{(p-1)/2} \equiv 1 \bmod p.$$

Si $b^p \equiv -b \bmod pS$, alors $b^{p-1} \equiv -1 \bmod pS$, et

$$b^2 \equiv 2 \bmod p \Rightarrow 2^{(p-1)/2} \equiv (b^2)^{(p-1)/2} \equiv b^{p-1} \equiv -1 \bmod pS \Rightarrow 2^{(p-1)/2} \equiv -1 \bmod p.$$

Cours N°7. Jeudi le 20 novembre 2003

8.7 Nombres pseudopremiers d'Euler

Rappels : Congruence d'Euler

PROPOSITION 8.3.1 *Soit n un nombre premier impair. Alors on a la congruence (8.2) :*

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \bmod n. \tag{8.2}$$

DÉFINITION 8.7.1 *Un nombre naturel n est appellé un* nombre pseudopremier de Euler par rapport à *a si* $\text{pgcd}(a,n) = 1$ *et (8.2) soit satisfaite.*

Si n n'est pas nécessairement premier, la congruence (8.2) peut être utilisée comme une condition de primalité si l'on définit le symbole de Jacobi à droite par la multiplicativité : pour un nombre impair positif $n = p_1 p_2 \dots p_k$, où p_i sont premiers (non nécessairement différents) posons

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_k}\right) \tag{8.20}$$

En effet, le symbole de Jacobi peut être étendu sur toutes les valeurs du "numérateur" et du "dénominateur" et il peut être calculé sans connaissance de la factorisation en produit des nombres premières de n.

Maintenant on va démontrer, en utilisant le théorème chinois (voir théorème 8.7.2), que si n est un nombre pseudopremier d'Euler par rapport à tout $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ alors n est premier. C'est à dire, il n'y a pas d'analogues eulériens des nombres de Carmichael.

THÉORÈME 8.7.2 (SOLOWAY-STRASSEN) *Un nombre impair n est premier si et seulement si pour tout a avec* $\text{pgcd}(a,n) = 1$,

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \bmod n. \tag{8.21}$$

PREUVE (voir [Dem], p. 125).

I) On suppose qu'il existe un nombre premier p impair tel que $p^2|n$, et on utilise le morphisme surjectif de groupes multiplicatifs

$$(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/p^2\mathbb{Z})^\times, \tag{8.22}$$

où le groupe $(\mathbb{Z}/p^2\mathbb{Z})^\times$ est cyclique d'ordre $p(p-1)$. Ceci implique (par la surjectivité) qu'il existe $\overline{a} \bmod n$ tel que

$$\begin{aligned} &p(p-1) \text{ divise } \text{ord}(\overline{a}) \Rightarrow p \text{ divise } \text{ord}(\overline{a})^{(n-1)/2} = \frac{\text{ord}(\overline{a})}{\text{pgcd}((n-1)/2, \text{ord}(\overline{a}))} \\ &\Rightarrow (\overline{a})^{(n-1)/2} \not\equiv \pm 1 \bmod n. \end{aligned}$$

(ou bien : $n = p^2 m$; $a = 1 + mp \Rightarrow \overline{a}^{n-1} \neq 1$, car $\overline{a}^p = 1$. En effet, $(1+mp)^p = 1 + p \cdot mp + \dots \equiv 1 \bmod n$ implique $\overline{a}^{n-1} = \overline{a}^n \overline{a}^{-1} = \overline{a}^{-1} \neq 1$).

II) Soit $n = p_1 \cdot \ldots \cdot p_r$ distincts, et $r \geq 2$,

$$(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \prod_{i=1}^{r} (\mathbb{Z}/(p_i))^\times.$$

Supposons qu'il existe un a tel que

$$a^{(n-1)/2} \equiv -1 \bmod n.$$

L'existence d'un tel a est nécessaire pour la congruence (8.21) puisque le théorème chinois permet de trouver, pour un choix arbitraire de $\eta_i = \pm 1$, un a avec

$$\left(\frac{a}{p_i}\right) = \eta_i, \tag{8.23}$$

donc on choisit $\prod_{i=1}^{r} \eta_i = -1$, puisque

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right)$$

Notons a_i la classe de a modulo p_i. On a d'une part,

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \cdot \ldots \cdot \left(\frac{a}{p_r}\right) = \left(\frac{a_1}{p_1}\right) \cdot \ldots \cdot \left(\frac{a_r}{p_r}\right)$$

D'autre part, réduisant modulo p_1 l'égalité initiale, on obtient

$$\left(\frac{a_1}{p_1}\right) \cdot \ldots \cdot \left(\frac{a_r}{p_r}\right) \equiv a_1^{(n-1)/2} \bmod p_1.$$

D'après le théorème chinois, on peut choisir les différentes a_i indépendamment. Mais le second membre ne dépend que de a_1, tandis qu'on peut changer le signe du premier sans modifier a_1, par exemple en modifient a_r. Cela est absurde et contrédit l'hypothèse $r \geq 2$.

8.8 Loi de réciprocité quadratique et tests de primalité.

Dans des tests modernes de primalité (Soloway-Strassen, Miller-Rabin...) on utilise la congruence (8.2) et le théorème 8.7.2. Ces tests de primalité, marchent beaucoup plus rapidement que toutes les méthodes connues de factorisation des grands nombres premiers "aléatoires".

Test de primalité de Soloway-Strassen

C'est un test probabiliste. Selon Emile Borel, "Un phénomène dont la probabilité est 10^{-50}, ne se produira donc jamais ou du moins ne sera jamais observé ("La probabilité et la vie").

Rappelons qu'un nombre naturel n est appellé un *nombre pseudopremier de Euler par rapport à a* si $\text{pgcd}(a, n) = 1$ et (8.2) soit satisfaite. Si (8.2) n'est pas satisfaite pour un a avec $\text{pgcd}(a, n) = 1$, alors n n'est pas premier, et on appelle a un témoin d'Euler de non-primalité de n. Selon le théorème 8.7.2, il existe toujours un témoin d'Euler de non-primalité d'un nombre composé impair n, mais la question qui reste est qu'il est le plus petit valeur de a, ou qui est la proportion de tels temoins.

Le test de primalité de Soloway-Strassen est basé sur l'observation suivante :

REMARQUE 8.8.1 *Soit n un nombre imaire. Si (8.2) n'est pas satisfaite pour un a avec* $\text{pgcd}(a, n) = 1$, *alors elle n'est pas satisfaite pour au moins de 50 % de a.*

En effet, soit $H = \{a_1, a_2, \cdots, a_j, \cdots\}$ l'ensemble de tous les $a = a_j$ pour lesquels (8.2) est satisfaite :

$$a_j^{(n-1)/2} \equiv \left(\frac{a_j}{n}\right) \bmod n. \tag{8.2}$$

Alors H est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^*$ donc $a \notin H \Rightarrow aH \cap H = \emptyset$, ceci dit, la condition (8.2) n'est pas satisfaite pour au moins de 50 % de a.

Description d'algorithme. Soit n impair. On choisit au hasard k nombres b, $0 < b < n$. Pour tout b on calcul les deux parties de la congruence d'Euler (8.2), $b^{(n-1)/2} \bmod n$ et $\left(\frac{b}{n}\right)$.

Le calcul de $b^{(n-1)/2} \bmod n$ coûte $\mathcal{O}(\log^3 n)$ opération bouléennes par la méthode de carrés successifs.

Le calcul de $\left(\frac{b}{n}\right)$ coûte $\mathcal{O}(\log^3 n)$ opération bouléennes à l'aide de la loi de réciprocité quadratique en utilsant divisions euclidiennes.

Si (8.2) est valable pour k choix au hasard de b, alors la probabilité du fait que n est composé en dépit d'avoir passé k tests avec succès, est inférieure ou égale à $1/2^k$, donc pour $k \sim 167$ on obtient une probabilité suffisante (selon E.Borel) :

$$2^{167} \approx 10^{50} \cdot 1.87072209578355573530071658 8.$$

Test conditionnel de primalité de Miller

Ce test utilise le fait d'existence d'un témoin d'Euler relativement petit.

Cependant, pour le montrer, on a besoin de l'Hypothèse de Riemann généralisée.

Soit $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ un caractère de Dirichlet (c'est à dire, un morphisme de groupes $(\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}$), et on pose pour $a \in \mathbb{Z}$, $\chi(a) = \chi(a \bmod N)$ pour $(a, N) = 1$ et $\chi(a) = 0$ pour $(a, N) > 1$. On considère la fonction L de Dirichlet

$$L(s, \chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s}$$

qui converge absoluement et ne s'annule pas pour $\mathrm{Re}(s) > 1$. Elle admète un prolongement analytique sur tout le plan complexe.

Hypothèse de Riemann généralisée. Pour toute fonction L de Dirichlet $L(s, \chi)$ on a

$$L(s, \chi) = 0, \mathrm{Re}(s) > 0 \Rightarrow \mathrm{Re}(s) = \frac{1}{2}.$$

Théorème 8.8.2 (G.Miller) *Supposons que pour tout $b < 2\log^2 n$ la condition (8.2) soit satisfaite, et que l'Hypothèse de Riemann généralisée soit valable.*

Alors n est premier.

Description de l'algorithme de Miller

On vérifie la condition de la congruence d'Euler (8.2),

$$b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \bmod n$$

pour tout $b < 2\log^2 n$. Si n passe tous ces tests, il est premier (conditionnel). L'analyse simple de coût T de cet algorithme montre que $T = \mathcal{O}(\log^5 n)$.

Remarque. On a observé récemment des "preuves" numériques que pour n composé il existe un témoine $a \leq 2\log n \log\log n$ tel que n pour que n soit un nombre pseudopremier d'Euler par rapport à a.

Pseudopremiers forts et le test de primalité de Miller-Rabin

On peut encore améliorer la condition de la congruence d'Euler (8.2),

$$b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \bmod n$$

qui est valable pour un nombre premier n. On remarque que dans le groupe cyclique $(\mathbb{Z}/n\mathbb{Z})^*$ les seules racines carrés de 1 sont ± 1. Cette condition, qui n'est pas suffisante pour la primalité d'un nombre impaire n, peut être utilisée comme une condition efficace probabiliste de primalité.

Définition 8.8.3 *Un nombre naturel n est appellé un* nombre pseudopremier fort par rapport à b *si* $\text{pgcd}(b,n)=1$ *et (8.2), et pour la présentation* $n-1=2^s t$ *avec* t *impair, il existe un* r, $0 \leq r < s$ *tel que*

$$b^{2^r t} \equiv -1 \bmod n.$$

Théorème 8.8.4 (Miller-Rabin)

(a) Soit n un nombre impaire composé, alors n n'est pas un nombre pseudopremier fort par rapport à b au moins de 75 % de b.

(b) Tout pseudopremier fort par rapport à b est un pseudopremier d'Euler par rapport à b.

Preuve (voir [Kob87], p.117, V.1.6, V.1.7).

Description de l'algorithme de Miller-Rabin On choisit au hasard k nombres b, $0 < b < n$. Pour tout b on vérifie les condition que n est un nombre pseudopremier fort par rapport à b : on calcule

$$b^{2^r t} \bmod n, \quad 0 \leq r < s$$

jusqu'on obtient $-1 \bmod n$.

Le calcul coûte $\mathcal{O}(\log^3 n)$ opération bouléennes seulement par la méthode de carrés successifs.

Si n est passé ces k tests pour k choix au hasard de b, alors la probabilité du fait que n est composé en dépit d'avoir passé k tests avec succès, est inférieure ou égale à $1/4^k$.

Remarque. On peut vérifier que $n = 3215031751$ est le seul nombre composé $n \leq 2.5 \cdot 10^{10}$ qui est pseudopremier fort pour $b = 2, 3, 5, 7$

```
? factor(3215031751)
%1 =
[151 1]

[751 1]

[28351 1]
```

Test polynômial déterministe de primalité de Agrawal, Kayal et Saxena ("PRIMES is in P", 2002)

Ce test utilise une version polynômiale de la condition nécessaire du petit théorème de Fermat, et il arrive qu'une telle version et suffisante et qu'elle amène à un algorithme très éfficace polynômial de primalité, voir une jolie exposition dans F.Bornemann, PRIMES is in P, une avancée accessible à "l'homme ordinaire" ", Gazette des mathématiciens, SMF, No 98, octobre 2003, pp. 14–30.

Exercices

8.1 Si p est un nombre premier, et $p \equiv \bmod 4$, montrer que

$$-1 \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \bmod p.$$

[Indication : En considérant $X^{p-1}-1$ dans $(\mathbb{Z}/p\mathbb{Z})[X]$ montrer d'abord que $(p-1)!+1 \equiv 0 \bmod p$].

8.2 713 est-il un carré modulo $p = 1009$?

8.3 (a) Soit $p = 2^{2^n}+1$ un nombre de Fermat premier, avec $n \geq 2$. Montrer que a est une racine primitive modulo p si et seulement si $\left(\frac{a}{p}\right) = -1$. Motrer que 3, 5 et 7 sont racines primitives modulo p.

(b) Montrer le critère de Pépin :

$$p = 2^{2^n}+1 \text{ est un nombre premier} \Longleftrightarrow 3^{(p-1)/2} \equiv -1 \bmod p.$$

8.4 Montrer que 2 est racine primitive modulo les premiers de la forme $4q+1$ ou $2q+1$ avec q premier, $q \equiv 1 \bmod 4$. Et si $p = 2q+1$ avec q premier, $q \equiv 3 \bmod 4$?

8.5 Calculer de tête les symbols : $\left(\frac{3}{97}\right)$, $\left(\frac{5}{389}\right)$, $\left(\frac{2003}{11}\right)$, et $\left(\frac{5!}{7}\right)$.

8.6 Montrer que pour un nombre premier $p \geq 5$ on a $\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1, 11 \pmod{12}, \\ -1 & \text{si } p \equiv 5, 7 \pmod{12}. \end{cases}$

8.7 Montrer qu'il n'y a pas de racines primitives modulo 2^npour tout $n \geq 3$.

8.8 Montrer que si p est un nombre premier, alors il existe une racine primitive modulo p^2. [Indication : Ecrire un élément de $(\mathbb{Z}/p^2\mathbb{Z})^*$ sous la forme du produit de deux élément. Rappeler que si a, b sont d'ordres n, m, avec $\text{pgcd}(n, m) = 1$, alors ab est d'ordre nm.]

8.9 En utilsant le fait que $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique montrer directement que $\left(\frac{-3}{p}\right) = 1$ pour $p \equiv 1 \pmod 3$. [Indication : Il existe un élément $c \in (\mathbb{Z}/p\mathbb{Z})^*$ d'ordre 3. Montrer que $(2c+1)^2 = -3$.]

8.10 Si $p \equiv 1 \pmod 5$, montrer directement que $\left(\frac{5}{p}\right) = 1$ par la méthode d'exercice 9. [Indication : Soit $c \in (\mathbb{Z}/p\mathbb{Z})^*$ un élément d'ordre 5. Montrer que $(c + c^4)^2 + (c + c^4) - 1 = 0$, etc.]

8.11 Pour quels nombres premiers p on a $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$?

8.12 Combien de nombres naturels $x < 2^{13}$ satisont l'équation

$$x^2 \equiv 5 \pmod{2^{13} - 1}?$$

(On peut utiliser le fait que $2^{13} - 1$ est premier.)

8.13 Trouver un nombre naturel $x < 97$ tel que $x \equiv 4^{48} \pmod{97}$.

8.14 Soit $n = p_1 \cdot \ldots \cdot p_r$ distincts, et $r \geq 2$, et soit a tel que

$$a^{(n-1)/2} \equiv -1 \bmod n.$$

Posons $n - 1 = 2^s t$ avec t impaire,et soit $p|n$, $p - 1 = 2^{s'} t'$ avec t' impaire.
Montrer que

$$s' \geq s, \text{ et } \left(\frac{a}{p_i}\right) = \varepsilon_i = \begin{cases} -1, & \text{si } s = s' \\ 1, & \text{si } s < s' \end{cases}, \tag{8.24}$$

Solution : On suppose, par l'absurde, $s' < s$, alors

$$a^{(n-1)/2} = a^{2^{s-1}t} \equiv -1 \bmod n \Rightarrow$$

$$a^{2^{s-1}t} \equiv (a^{2^{s-1}t})^{t'} \equiv a^{2^{s-1}t'} \equiv -1 \bmod n \Rightarrow a^{2^{s-1}t'} \equiv -1 \bmod p,$$

puisque t et t' sont impaires. Ensuite, l'hypothèse $s' < s$ implique

$$a^{2^{s'}t'} \equiv 1 \bmod p \Rightarrow a^{2^{s-1}t'} \equiv 1 \bmod p,$$

et on a une contradiction avec la congruence précédente $a^{2^{s-1}t'} \equiv -1 \bmod p$.

- Cas $s' = s$: $\left(\frac{a}{p}\right) = a^{(p-1)/2} = a^{2^{s'-1}t'} \equiv -1$
  puisque $(a^{2^{s'-1}t})^{t'} \equiv -1 \bmod p$.

- Cas $s' > s$:

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} = a^{2^{s'-1}t'} \equiv (a^{2^{s'-1}t'})^{2^{s'-1}} \equiv 1 \bmod p. \qquad \square$$

8.15 Sur l'anneau $\mathbb{Z}/N\mathbb{Z}$, il existe aussi un analogue de la fonction bêta :

$$B(s,t) = \int_0^1 x^{s-1}(1-x)^{t-1}dx =$$

$$\int_{\mathbb{R}_+^\times} \frac{y^s}{(1+y)^{s+t}} \frac{dy}{y} \ (\mathrm{Re}(s), \mathrm{Re}(t) > 0).$$

Il est appellé somme de Jacobi de deux caractères de Dirichlet $\chi, \psi \bmod N$. Par la définition

$$J(\chi,\psi) = \sum_{x \bmod N} \chi(x)\psi(1-x) = \sum_{y \bmod N} \chi(y)\overline{(\chi\psi)}(1+y).) \tag{8.25}$$

En utilisant le changement de variables $y(1-x) \mapsto x$, $x(1+y) \mapsto y$), démontrer l'égalité entre les deux expressions

8.16 En supposant χ, ψ, et $\chi\psi$ tous primitifs modulo N, montrer que

$$J(\chi,\psi) = G(\chi)G(\psi)/G(\chi\psi) = J(\psi,\chi) \tag{8.26}$$

correspondant à l'identité classique $B(s,t) = \Gamma(s)\Gamma(t)/\Gamma(s+t)$.

Solution : si l'on calcule le produit

$$G(\chi)G(\psi) = \sum_{x \bmod N} \chi(x)\zeta_N^x G(\psi) = \sum_{x \bmod N} \chi\psi(x)\zeta_N^x \overline{\psi(x)} G(\psi). \tag{8.27}$$

En appliquant (8.13), on obtient

$$\overline{\psi(x)}G(\psi) = G_x(\psi) = \sum_{y \bmod N} \zeta_N^{xy}\psi(y)$$

et (8.27) se transforme en

$$\sum_{x,y \bmod N} (\chi\psi)(x)\psi(y)\zeta_N^{x(1+y)} = \sum_{y \bmod N} \psi(y)G_{1+y}(\chi\psi) =$$
$$\sum_{y \bmod N} \psi(y)\overline{(\chi\psi)}(1+y)G(\chi\psi) = J(\psi,\chi)G(\chi\psi). \tag{8.28}$$

9 Rappels sur la notion de corps, exemples

Nous avons déjà vu :

Définition 4.2.4

Un corps *est un anneau commutatif A, non réduit à $\{0\}$ dans lequel tout élément non-nul est inversible :*

Corps $\forall x \in A, x \neq 0, \exists y \in A, xy = 1$

Proposition 4.2.5

(a) Soit A un corps, alors A est un anneau intégre.

(b) Soit A un corps, I un idéal de A. Alors soit $I = \{0\}$ soit $I = A$.

Exemple.

On note par $\mathbb{Z}$ l'anneau des entiers relatifs,
$\mathbb{Q}$ le corps des nombres rationnels,
$\mathbb{R}$ le corps des nombres réels et
$\mathbb{C}$ le corps des nombres complexes.

9.1 Corps des fractions

PROPOSITION 9.1.1 *Si A est un anneau intégre, alors il existe un corps K appelé* corps des fractions *de A et noté $Frac(A)$ tel que*

(i) $A \subset K$;

(ii) Pour tout corps L et tout morphisme d'anneaux injectif $\phi : A \to L$, il existe un unique morphisme de corps $\psi : K \to L$ tel que $\psi|_A = \phi$.

PREUVE. Construction. On définit sur $A \times A\backslash\{0\}$ la relation $\mathcal{R}$ par

$$(a, b)\mathcal{R}(c, d) \iff ad = bc.$$

On vérifie en utilisant l'intégrité de A que $\mathcal{R}$ est une relation d'équivalence. On note K l'ensemble quotient $A \times A\backslash\{0\}/\mathcal{R}$, et $\frac{a}{b}$ l'image de (a, b) dans ce quotient. L'application de A dans K qui envoie a sur $(a, 1) = \frac{a}{1}$ est injective, et on identifie A avec son image. On muni alors K des lois

$$+ : K \times K \to K, (\frac{a}{b}, \frac{c}{d}) \mapsto \frac{ad + bc}{bd} \in K \quad (\text{"}addition\text{"});$$
$$\times : K \times K \to K, (\frac{a}{b}, \frac{c}{d}) \mapsto \frac{ac}{bd} \in K \quad (\text{"}multiplication\text{"});$$

On vérifie que ces lois sont bien définies et munissent K d'une structure de corps, l'élément neutre pour l'addition étant $0/1$, l'élément neutre pour la multiplication étant $1/1$, et l'inverse d'un élément non nul $\frac{a}{b}$ étant $\frac{b}{a}$.

Proprieté universelle. Soit L un corps et $\phi : A \to L$ un morphisme d'anneaux injectif il existe un unique morphisme de corps $\psi : K \to L$ tel que $\psi|_A = \phi$, l'application

$$A \times A\backslash\{0\} \to L, \frac{a}{b} \mapsto \frac{\phi(a)}{\phi(b)} \in L$$

passe au quotient et définit un morphisme de corps $K \to L$ qui convient. D'un autre coté, si ψ est un tel morphisme de corps, alors $\psi(a/b) = \frac{\psi(a)}{\psi(b)}$, ce qui montre l'unicité de ψ.

9.2 Caractéristique d'un corps, sous-corps premier

DÉFINITION 9.2.1 *Si A est un anneau commutatif, il existe un unique morphisme d'anneaux $\phi : \mathbb{Z} \to A$, donné par $\phi(n) = n \cdot 1$. Son noyau, $\mathrm{Ker}\phi$, est un sous-groupe de $\mathbb{Z}$. Le générateur positif de ce sous-groupe est appelé la* caractéristique *de A et est noté $car(A)$.*

PROPOSITION 9.2.2 *La caractéristique d'un corps K est nul ou un nombre premier $p = car(K)$. Si la caractéristique du corps est nulle, celui-ci contient un sous-corps, isomorphe à $\mathbb{Q}$. Sinon, il contient un sous-corps, isomorphe à $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, où p est sa caractéristique. Le corps ainsi obtenu est le plus petit corps contenu dans K, on l'appelle sous-corps premier de K.*

9.3 Modules et espaces vectoriels

DÉFINITION 9.3.1 *Si A est un anneau commutatif. Un A-module est la donnée d'un groupe abélien M, muni d'une loi externe*

$$\times : A \times M \to M, (a, m) \mapsto am \in M \quad (\text{"}multiplication\ externe\text{"})$$

satisfaisant les propriétés suivantes :

Mo1 $\forall a \in A,\ \forall x, y \in M,\ a(x+y) = ax + ay,$
Mo2 $\forall a, b \in A,\ \forall x \in M,\ (a+b)x = ax + bx,$
Mo3 $\forall a, b \in A,\ \forall x \in M,\ a(bx) = (ab)x.$
Si K est un corps un espace vectoriel sur K est un K-module.

EXEMPLE. La notion de $\mathbb{Z}$-module coïncide avec celle de groupe abélien :

$$\times : \mathbb{Z} \times M \to M, (a, m) \mapsto am \in M$$

EXEMPLE 9.3.2 *Si A est un anneau commutatif, et $n \in \mathbb{N}$, A^n est un A-module pour la lois externe*

$$\times : A \times A^n \to A^n, (a, (a_1, \cdots, a_n) \mapsto (aa_1, \cdots, aa_n) \in A^n$$

EXEMPLE 9.3.3 *Soit A est un anneau commutatif, et soit M un A-module. Si X est un ensemble, alors pour tout $a \in A$ et pour toute application $f : X \to M$ on pose*

$$\forall x \in X, (af)(x) = a(f(x)) \in M.$$

L'ensemble M^X de toutes les applications $f : X \to M$ est un A-module avec la loi externe

$$\times : A \times M^X \to M^X, (a, f) \mapsto af \in M^X$$

DÉFINITION 9.3.4 *Soit A est un anneau commutatif, et soient M, N deux A-modules. Une application $\phi : M \to N$ est dit un* morphisme *de A-modules (ou une application A-linéaire) si c'est un morphisme de groupe abéliens, et si elle vérifie la condition suivante :*

Mor. $\forall \lambda \in A, \forall m \in M, \phi(\lambda m) = \lambda \phi(m)$

Un isomorphisme de A-modules est un morphisme A-modules qui est bijectif. Son inverse est alors un morphisme A-modules.

Sous-A-modules, sous-espaces vectoriels

DÉFINITION 9.3.5 *Soit A est un anneau commutatif, et soient M un A-module. Un sous-groupe abélien $N \subset M$ est dit un sous-A-module si il vérifie la condition suivante :*

Sous $-$ module $\forall \lambda \in A, \forall x \in N, \lambda x \in N.$

Si K est un corps, un sous-K-module d'un espace vectoriel sur K est dit un sous-espace vectoriel sur K.

EXEMPLE 9.3.6 *Soit A est un anneau commutatif, et soient M, N deux A-modules. L'ensemble $\mathcal{L}(M, N)$ des applications A-linéaires $\phi : M \to N$ est un sous-A-module du module N^M de toutes les applications de M vers N. En particulier, si K est un corps, et E un K-espace vectoriel, le dual de E, noté $E^\vee$ est l'espace vectoriel $\mathcal{L}(E, K)$.*

9.4 Rappels sur les espaces vectoriels

DÉFINITION 9.4.1 *Soit K un corps. Une famille $(a_i)_{i\in I}$ d'éléments de K est dite* présque nulle *si et seulement si l'ensemble*

$$\{i \in I \mid a_i \neq 0\}$$

est fini.

Soient E un espace vectoriel sur K et $\mathbf{e} = (e_i)_{i\in I}$ une famille d'éléments de E. La famille $\mathbf{e}$ est

- *une famille* génératrice *si et seulement si pour tout x de E, il existe une famille présque nulle $(a_i)_{i\in I}$ d'éléments de K tels que*
$$x = \sum_{i\in I} a_i e_i$$
- *une famille* libre *si et seulement si pour toute famille présque nulle $(a_i)_{i\in I}$ d'éléments de K, on a tels que*
$$\sum_{i\in I} a_i e_i = 0 \Rightarrow \forall i \in I, a_i = 0$$
On dit alors que les éléments de $(e_i)_{i\in I}$ sont linéairement indépéndants
- *une* base *de E si elle est à la fois* libre *et* génératrice*. Pour tout x de E, il existe alors une seule famille présque nulle $(a_i)_{i\in I}$ d'éléments de K tels que*
$$x = \sum_{i\in I} a_i e_i.$$
On dit que $(a_i)_{i\in I}$ sont les coordonnées *de x en base $\mathbf{e}$.*

THÉORÈME 9.4.2 (SUR L'EXISTENCE D'UNE BASE) *Si E est un espace vectoriel sur K, alors il existe une base de E. Toutes les bases ont le même cardinal appelé dimension de E et noté* $\dim E$.

On ne donne pas de démonstration ici, mais on remarque :

PROPOSITION 9.4.3 *Soit K un corps. Soient E un espace vectoriel sur K et $\mathbf{e} = (e_i)_{i\in I}$ une famille d'éléments de E. Les conditions suivantes sont équivalentes :*

- *(i) la famille $\mathbf{e}$ est une* base *de E,*
- *(ii) la famille $\mathbf{e}$ est une famille* génératrice *et toute sous-famille de $\mathbf{e}$ distincte de $\mathbf{e}$ n'est pas* génératrice
- *(iii) la famille $\mathbf{e}$ est une famille* libre *et toute famille contenant $\mathbf{e}$ distincte de $\mathbf{e}$ n'est pas* libre

DÉFINITION 9.4.4 *Un espace vectoriel E sur K est dit de* dimension finie*, si et seulement s'il admet une famille* génératrice finie

THÉORÈME 9.4.5 *Si E est un espace vectoriel sur K de* dimension finie*, toutes les bases de E ont le même cardinal appelé dimension de E et noté* $\dim E$*. En outre :*

- *(i) une famille génératrice a au moins* $\dim E$ *composantes, et est une base si elle en a exactement* $\dim E$*,*
- *(ii) une famille* libre *a au plus* $\dim E$ *composantes, et est une base si elle en a exactement* $\dim E$.

EXEMPLE 9.4.6 *Si E est un espace vectoriel sur K de dimension finie, et si $(e_1, \cdots, e_n)$ une base de E, alors $E^\vee$ est un espace vectoriel de dimension finie, une base étant donnée par $(e_1^\vee, \cdots, e_n^\vee)$ où $e_i^\vee$ est définie par*

$$\forall (a_1, \cdots, a_n) \in K^n,\ e_i^\vee(a_1 e_1 + \cdots + a_n e_n) = a_i \in K.$$

Cette base $(e_1^\vee, \cdots, e_n^\vee)$ est appelée la base dual *de $(e_1, \cdots, e_n)$.*

9.5 Matrices de changement de bases

DÉFINITION 9.5.1 *Soit E est un K-espace vectoriel de dimension finie et soient $\mathbf{e} = (e_1, \cdots, e_n)$, $\mathbf{e}' = (e'_1, \cdots, e'_n)$ deux bases de E.*

La matrice

$$P = P_{\mathbf{e}}^{\mathbf{e}'} = (p_{ij}), p_{ij} = e_i^{\vee}(e'_j) \in K$$

qui a pour j-ème colonne les coordonnées de e'_j dans la base $(e_1, \cdots, e_n)$, est appelée matrice de changement de bases.

PROPOSITION 9.5.2

(i) Soit x un élément d'un K-espace vectoriel E de dimension finie et soient $\mathbf{e} = (e_1, \cdots, e_n)$, $\mathbf{e}' = (e'_1, \cdots, e'_n)$ deux bases de E.

On pose

$$x = x_1 e_1 + \cdots + x_n e_n,\ x = x'_1 e'_1 + \cdots + x'_n e'_n,$$

Alors

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = P_{\mathbf{e}}^{\mathbf{e}'} \begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix}$$

où $P_{\mathbf{e}}^{\mathbf{e}'}$ est matrice de changement de bases.

(ii) On a les relations

$$P_{\mathbf{e}}^{\mathbf{e}'} P_{\mathbf{e}'}^{\mathbf{e}''} = P_{\mathbf{e}}^{\mathbf{e}''} \text{ et } {P_{\mathbf{e}}^{\mathbf{e}'}}^{-1} = P_{\mathbf{e}'}^{\mathbf{e}}.$$

DÉFINITION 9.5.3 *Soit $\phi : E \to E$ une application linéaire d'un K-espace vectoriel E de dimension finie vers E, et soit $\mathbf{e} = (e_1, \cdots, e_n)$ une bases de E.*

La matrice

$$A = A_{\phi,\mathbf{e}} = (a_{ij}), p_{ij} = e_i^{\vee}(\phi(e_j)) \in K$$

qui a pour j-ème colonne les coordonnées de $\phi(e_j)$ dans la base $(e_1, \cdots, e_n)$, est appelée matrice de l'application linéaire dans la base donnée.

PROPOSITION 9.5.4

(i) Soit $\phi : E \to E$ une application linéaire d'un K-espace vectoriel E de dimension finie vers E, et soient $\mathbf{e} = (e_1, \cdots, e_n)$, $\mathbf{e}' = (e'_1, \cdots, e'_n)$ deux bases de E.

On pose

$$x = x_1 e_1 + \cdots + x_n e_n,\ x = x'_1 e'_1 + \cdots + x'_n e'_n,$$
$$\phi(x) = y_1 e_1 + \cdots + y_n e_n,\ \phi(x) = y'_1 e'_1 + \cdots + y'_n e'_n,$$

Alors

$$\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = A_{\phi,\mathbf{e}} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

où $A_{\phi,\mathbf{e}}$ est matrice de l'application linéaire dans la base donnée.

(ii) On a les relations

$$A_{\phi,\mathbf{e}'} = {P_{\mathbf{e}}^{\mathbf{e}'}}^{-1} A_{\phi,\mathbf{e}} P_{\mathbf{e}}^{\mathbf{e}'}.$$

9.6 Caractères d'un groupe

DÉFINITION 9.6.1 *Etant donné un groupe G et on corps K, on appelle* caractère *de G dans K tout mophisme de groupes de G dans K^*.*

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

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

EXEMPLE 9.6.2 *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'exponentuelle 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 9.6.3 (D'INDÉPENDANCE LINÉAIRE DE CARACTÈRES) *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'était 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 linairement 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 $a_2 = \cdots = a_n$, ce qui prouve que $\sigma_1, \cdots, \sigma_n$ sont linéairement indépendants.

COROLLAIRE 9.6.4 *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 9.6.3.

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

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

PROPOSITION 9.6.5 *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 9.6.6 *Si G est un groupe fini, la famille $(\chi)_{\chi \in X^*(G)}$ est une famille libre du $\mathbb{C}$-espace vectoriel $\mathbb{C}^G$*

Cours N°8. Jeudi le 27 novembre 2003

10 Extensions.

10.1 Polynômes irréductibles.

DÉFINITION 10.1.1 *Soit K un corps. Un polynôme $f \in K[X]$ est dit* irréductible, *si et seulement si il vérifie les deux conditions suivantes :*

Irr1. $f \notin K$

Irr2. *Si $f = gh$ avec $g, h \in K[X]$ alors $g \in K^\times$ ou $h \in K^\times$.*

EXEMPLE 10.1.2 *Soit K un corps.*

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

(ii) Un polynôme $f \in K[X]$ 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 10.1.3 (CRITÈRE D'IRRÉDUCTIBILITÉ) *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.*

Rappels : division des polynômes avec reste sur un anneau et sur un corps

PROPOSITION 7.2.1. *Soit A un anneau commutatif intègre. On se donne un polynôme $P(X) = \sum_{i=0}^{d} a_i X^i$ à coefficients dans A telle que a_d soit un élément inversible de A. Alors pour tout polynôme $f(X)$ de $A[X]$ il existe une unique paire $(Q, R) \in A[X]^2$ telle que*

$$f = PQ + R \text{ avec } R = 0 \text{ ou } \deg R < \deg P.$$

THÉORÈME 7.2.2. *Soit K un corps. Pour tous polynômes $f(X)$ et $P(X)$ tels que $P(X)$ soit non nul à coefficients dans un corps K il existe une unique paire $(Q, R) \in K[X]^2$ telle que*

$$f = PQ + R \text{ avec } R = 0 \text{ ou } \deg R < \deg P.$$

Rappels : anneaux euclidiens et anneaux principaux

Nous avons vu que l'anneau $K[X]$ des polynômes sur un corps K est euclidien, et donc factoriel :

DÉFINITION 4.5.1. *Un anneau intègre A est dit* euclidien *s'il existe une application $\phi : A \in \mathbb{N}$ appelée* stathme *telle que*

$$\forall a \in A \backslash \{0\} \forall b \in A, \exists (q, r) \in A^2, b = aq + r \text{ avec } r = 0 \text{ ou } \phi(r) < \phi(a)$$

EXEMPLE 10.1.4 . *Soit K un corps. L'anneau $K[X]$ est un anneau euclidien pour l'application $\phi : K[X] \backslash \{0\} \to \mathbb{N}$ de degré d'un polynôme : $\phi(f) = \deg(f)$.*

Rappels : caractérisation d'éléments irréductibles dans un anneau principal

On a vu que les éléments irréductibles de l'anneau $K[X]$ sont exactement les polynômes irréductibles :
DÉFINITION 10.1.1. *Un élément $a \in A$ est dit* irréductible, *si et seulement si il vérifie les deux conditions suivantes :*
Irr1. $a \notin A^\times$
Irr2. *Si $a = bc$ avec $a, b \in A$ alors $a \in A^\times$ ou $b \in A^\times$.*

DÉFINITION 4.5.2. *Un anneau intègre A est dit* principal *si tout idéal I de A est principal, c'est à dire, il existe un $a \in A$, tel que $I = (a)$.*

PROPOSITION 4.5.4 *Soit A un anneau principal. Les assertions suivantes sont équivalentes :*
(i) $\mathfrak{a}$ est un idéal maximal non nul de A ;
(ii) $\mathfrak{a}$ est un idéal premier non nul de A ;
(iii) il existe un élément p irréductible de A tel que $\mathfrak{a} = (p)$.

DÉFINITION 4.6.1. *Un anneau intègre A est dit* factoriel *si et seulement s'il vérifie les conditions suivantes :*
Existence. *Pour tout élément non nul a de A il existe un élément inversible $u \in A^\times$ et des éléments irréductibles $p_1, \cdots, p_m$ de A tels que*

$$a = up_1 \cdot \ldots \cdot p_m$$

(il se peut que $m = 0$, dans ce cas $a \in A^\times$).
Unicité. *Soient m, n, $p_1, \cdots, p_m$ et $q_1, \cdots, q_m$ des éléments irréductibles de A et $u, v \in A^\times$ des éléments inversibles de A tels que*

$$up_1 \cdot \ldots \cdot p_m = vq_1 \cdot \ldots \cdot q_n,$$

alors $m = n$ et il existe une permutation $\sigma \in \mathfrak{S}_n$ telle que $q_i \sim p_{\sigma(i)}$ pour $i = 1, \cdots n$.

THÉORÈME 4.5.3. *Tout anneau A euclidien est principal.*

THÉORÈME 4.6.2. *Tout anneau A principal est factoriel.*

10.2 Extensions, degré.

DÉFINITION 10.2.1
(i) Soit K un corps et L un autre corps, contenant K. On appelle L 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 note ce degré $[L : K]$, le degré est énentuellement infini. Si la dimension $\dim_K L$ est finie on appelle L 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 10.2.2 *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

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

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

COROLLAIRE 10.2.3 *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 10.2.4 *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,

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

10.3 Eléments algébriques

Soit E une extenstion d'un corps K.

DÉFINITION 10.3.1

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

(ii) Une extension E de K est dit 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 $f \in K[X]$ tels que $f(\alpha) = 0$, forment 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 10.3.2 *Soit E une extenstion d'un corps K, et soit α un élément de E algébrique sur K de polynôme minimal f.*

(i) Si $g \in K[X]$ admet α comme racine, alors f divise g dans $K[X]$.

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

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

(ii) Si f se décompose dans $K[X]$ sous la forme gh, dans le corps E, on a $f(\alpha) = g(\alpha)h(\alpha) = 0$, donc $g(\alpha) = 0$ ou $h(\alpha) = 0$, et f divise g ou h. □

PROPOSITION 10.3.3 *Soit E une extenstion finie d'un corps K ($[E : K] = n \in \mathbb{N}$), alors E est algébrique sur K.*

PREUVE.
Soit α un élément de E, alors la multiplication par α donne une application K-linéaire

$$\varphi_\alpha : E \to E, x \mapsto \alpha x.$$

Ensuite α est algébrique sur K parce que α est annulé par le polynôme caractèristique

$$f_\alpha(X) = \det(\varphi_\alpha - X\mathrm{Id}_E).$$

(selon le théorème de Cayley-Hamilton on a $f_\alpha(\varphi_a) = 0$ dans l'anneau $\mathrm{End}_K(E)$, donc $(f_\alpha(\varphi_\alpha))(1) = f_\alpha(\alpha) \cdot 1 = 0$ dans E.)

REMARQUE. L'assertion réciproque n'est pas valable, l'extension $E = \overline{\mathbb{Q}} \subset \mathbb{C}$ de $\mathbb{Q}$, formée par tous les nombres algébriques comlexes, est algébrique par la définition, mais $[E : K]$ n'est pas finie. En effet, on vérifie qu'il existe des polynômes irréductibles sur $\mathbb{Q}$ de degré arbitraire n, par exemple $X^n - 2$ (en exercice obligatoire).

10.4 Corps de rupture

Rappelons que pour un corps arbitraire K et pour tout polynôme $f(X) \in K[X]$ on peut toujours construire une extension L dans laquelle f possède une racine. On peut supposer $f(X)$ irréductible auquel cas on a vu que l'anneau quotient $K[X]/(f)$ est un corps (par l'algorithme d'Euclide). La classe $X + (f)$ est alors une racine de f dans $K[X]/(f)$.

THÉORÈME 10.4.1 (SUR L'ISOMORPHISME) *Soit $\alpha \in L$ une racine d'un polynôme irréductible $f(X)$. Alors l'anneau $K[\alpha]$ est un corps isomorphe à $K[X]/(f)$.*

En effet, si $0 \neq h(\alpha) \in K[\alpha]$, $h(X)$ et $f(X)$ sont premiers entre eux par irréductibilité de f. Alors il existe u, $v \in K[X]$ tels que $f(X)u(X) + h(X)v(X) = 1$. L'application

$$h(X) + (f) \mapsto h(\alpha)$$

est donc bien définie, et est un isomorphisme de corps.

DÉFINITION 10.4.2 *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 $P(\alpha) = 0$.*

PROPOSITION 10.4.3 *Soit K un corps, et f un polynôme irréductible. Alors l'anneau $K[X]/(f)$ est un corps de rupture de P sur K, où $\alpha = X + (f) \in L$ est tel que $L = K(\alpha)$ et $P(\alpha) = 0$.*

REMARQUE 10.4.4 *Soit K un corps, et P un polynôme irréductible. Alors on peut donner une construction matricielle de l'anneau $K[X]/(f)$ qui est un corps de rupture de P sur K, ici $\alpha = X + (f) \in L$ est tel que $L = K(\alpha)$ et $P(\alpha) = 0$.*

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

$$K[X]/(f) = \langle 1, X, \cdots, X^{n-1} \rangle \bmod (f)$$

la multiplication $\varphi : h \mapsto \overline{X}h \bmod (f)$ est donnée par la 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 minimale est égale à $f(X)$. Il vient que $K[A] \cong K[X]/\mathrm{Ker}(\varphi)$ est isomorphe à $K[X]/(f)$.

Cette construction implique aussi que pour tout polynôme $f(X) \in K[X]$ on peut trouver une extension finie L' dans laquelle f se décompose en produit de facteurs de premier degré. La construction implique que L peut être choisi de tel façon que $[L' : K] \leq n!$.

DÉFINITION 10.4.5 *On considère un polynôme $f(X) \in K[X]$ de degré supèrieur ou égal à 1, et une extension E de K, dans laquelle f s'écrit $f(X) = (X-\alpha_1)\cdot\ldots\cdot(X-\alpha_n)$. Alors le corps $L = K(\alpha_1, \cdots, \alpha_n)$ s'appelle* corps de décomposition *de f dans E. C'est une extension minimale de K dans E, dans laquelle f se décompose en produit de facteurs linéaires.*

On peut vérifier que ce corps est uniquement déterminé à un isomorphisme près.

THÉORÈME 10.4.6 (SUR UN PROLONGEMENT D'ISOMORPHISME) *On considère un isomorphisme de corps $\sigma : K \to K'$, et un polynôme irréductible $f = \sum_{j=0}^{n} a_j X^j \in K[X]$. On note $f^\sigma = \sum_{j=0}^{n} \sigma(a_j) X^j \in K'[X]$. On choisit une extension de K' contenant une racine β de f, et une extension de K', contenant une racine β' de $f^\sigma(X)$. 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 $\sigma : K \to K'$, l'application

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

est un isomorphisme d'anneaux. On en déduit

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

Cela montre à la fois que f^σ est un élément irréductible de $K'[X]$, et que si $\theta = h(\beta) \in K(\beta)$, son image par $\tilde{\sigma}$ est bien définie par l'égalité $\tilde{\sigma}(\theta) = h^\sigma(\beta')$, CQFD.

THÉORÈME 10.4.7 (DE L'UNICITÉ) *Soient $\sigma : K \xrightarrow{\sim} K'$ un isomorphisme de corps, un polynôme $f = \sum_{j=0}^{n} a_j X^j \in K[X]$, et $f^\sigma = \sum_{j=0}^{n} \sigma(a_j) X^j \in K'[X]$.*

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

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

$$\tau : B \to B',$$

dont la restriction à K est égale à σ.

PREUVE. Le polynôme f s'écrit $f(X) = a(X-\alpha_1)\cdot\ldots\cdot(X-\alpha_n)$, 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 p, et il existe $g \in K[X]$ tel que $f = pg$.

Dans $E'[X]$, on a les égalités

$$f^\sigma = p^\sigma g^\sigma = a'(X - \alpha'_1)\cdot\ldots\cdot(X - \alpha'_n).$$

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

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

donc il existe un indice i, qu'on peut supposer égal à 1, tel que $\beta = \alpha'_1 \in E'$. On utilise le théorème 10.4.6 pour le polynôme irréductible p : il existe un isomorphisme de corps

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

qui prolonge σ.

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

Le nombre de racines de f non dans 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 $L'(\alpha'_2, \cdots, \alpha'_n) = K'(\alpha'_1, \alpha'_2, \cdots, \alpha'_n)$, CQFD.

COROLLAIRE 10.4.8 (DE L'UNICITÉ) *Soient $\sigma : K \xrightarrow{\sim} K'$ un isomorphisme de corps, un polynôme $f = \sum_{j=0}^n a_j X^j \in K[X]$, et $f^\sigma = \sum_{j=0}^n \sigma(a_j) X^j \in K'[X]$.*

Alors le corps de décomposition de f est défini à isomorphisme près.

10.5 Sous-groupes finis dans K^*

Exposant d'un groupe commutatif fini

Soit G un groupe commutatif 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 tel que $x^{\omega(G)} = e$ pour tout élément $x \in |G|$. Soit K un corps, et $G \subset K^\times$ un sous-groupe fini. Alors par la définition de ppcm, et par le théorème de Lagrange, $\omega(G)||G|$, et tous les $x \in G$ sont les solutions de $x^{\omega(G)} = 1$, mais elle possède au plus $\omega(G)$ solutions. Donc, $\omega(G) = |G|$, et il reste à vérifer que dans tout groupe abélien G il existe un élément d'ordre $\omega(G)$.

Il suffit d'utiliser plusieures fois le résultat suivant :

LEMME 8.1.5. *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, et on suppose que* $\text{pgcd}(r, s) = 1$. *Alors ab est d'ordre rs.*

C'est un fait général sur les éléments d'un groupe qui commutent entre eux.

PREUVE (rappel). Lorsque $(ab)^{rs} = a^{rs}b^{rs} = 1$, 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 $a^{r_1r_2s_1} = (a^{r_1r_2})^{s_1} = 1$,

$$b^{r_1r_2s_1} = 1.$$

Ceci implique que $s \mid r_1r_2s_1$, et, car $\text{pgcd}(s, r_1r_2) = 1$, il vient que $s = s_1$. Un argument similaire montre que $r = r_1$, donc l'ordre de ab est rs.

LEMME 10.5.1 *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 $\text{ppcm}(r, s)$, 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 $\text{ppcm}(r, s)\text{pgcd}(r, s)=rs$. Par exemple, si

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

Une autre construction : notons $d = \text{pgcd}(r, s)$. Il s'agit de construire un diviseur s' de s qui soit premier à r/d. 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
```

$$i := 2$$

Alors $x^{r/r'}$ est d'ordre r', et $y^{s/s'}$ est d'ordre s', donc on peut appliquer le lemme 8.1.5.

Cyclicité des sousgroupes finies de $K^\times$

THÉORÈME 10.5.2 *Soit K un corps, et $G \subset K^\times$ un sous-groupe fini. Alors le groupe G est cyclique.*

PREUVE. Soit K un corps, et $G \subset K^\times$ un sous-groupe fini. Alors par la définition de ppcm, et par le théorème de Lagrange, $\omega(G)||G|$, et tous les $x \in G$ sont les solutions de $x^{\omega(G)} = 1$, mais ce polynôme possède au plus $\omega(G)$ racines. Donc, $\omega(G) = |G|$, et on a vu que dans tout groupe abélien G il existe un élément d'ordre $\omega(G)$.

EXERCICES

10.1 Soit K un corps. En considérant l'ordre des élément 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.

10.2 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 $\sum_{x \in K} x^s$.

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

10.4 Montrer qu'il existe des polynômes irréductibles sur $\mathbb{Q}$ de degré arbitraire n, par exemple $X^n - p$, p un nombre premier.

Cours N°9. Jeudi le 4 decembre 2003

11 Morphisme de Frobenius, structure des corps finis

Pour un plus large développement sur les corps finis le lecteur est renvoyé aux textes d'E.Peyre [Pey], ainsi que Lidl-Niederreiter, [Li-Ni].

11.1 Structure

PROPOSITION-DÉFINITION 11.1.1 *: Soit A un anneau commutatif de caractéristique p un nombre premier. L'application*

$$Fr_p : x \mapsto x^p, x \in A$$

est un morphisme d'anneau 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 $Fr_q : x \mapsto x^q$.

THÉORÈME 11.1.2 *: Soit $\mathcal{K}$ un corps fini. Alors $\mathcal{K}$ est de caractéristique p premier, $\mathcal{K}$ est de cardinal $q = p^d$, avec $d = [\mathcal{K} : \mathbb{F}_p]$. Inversement, si p est premier, 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 $\mathbb{F}_p$. On note ce corps $\mathbb{F}_q$. De plus, on a l'existence de deux isomorphismes : un de $(\mathbb{F}_q, +)$ sur $((\mathbb{Z}/p\mathbb{Z})^d, +)$ et un du groupe multiplicatif $\mathbb{F}_q^*$ sur $\mathbb{Z}/(q-1)\mathbb{Z}$ ($\mathbb{F}_q^*$ est un groupe cyclique d'ordre $q-1$).*

PREUVE. Vérifions d'abord q'un corps $\mathcal{K}$ à q éléments est un corps de décomposition pour le polynôme $X^q - X$. Comme $\mathcal{K}$ a q éléments, $\mathcal{K}^*$ est un groupe d'ordre $q-1$. Par conséquant,

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

Autrement dit tous les éléments de $\mathcal{K}$ sont racines de $X^q - X$. Comme ce polynôme a au plus q racines, on obtient

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

En particuler, $\mathcal{K}$ est un corps de décomposition pour le polynôme $X^q - X$.

Inversement soit $\mathcal{K}$ un corps de décomposition pour le polynôme $X^q - X$ sur $\mathbb{F}_p$. Comme Fr_q est un automorphisme de $\mathcal{K}$, l'ensemble des racines de $X^q - X$ est un sous-corps de $\mathcal{K}$. Comme $\mathcal{K}$ est engendré par ces racines, $\mathcal{K}$ est l'ensemble des racines de $P = X^q - X$. Comme $P' = -1$, toutes les racines de P sont d'ordre 1, il a donc toutes ses racines distinctes dans $\mathcal{K}$. Comme il est scindé dans $\mathcal{K}$, $\mathcal{K}$ a exactement q éléments.

L'assertion concernant le groupe additif résulte de la srtructure de $\mathbb{F}_q$ comme espace vectoriel. Celle sur la cyclicité du groupe $\mathcal{K}^*$ découle du théorème 10.5.2, CQFD.

THÉORÈME 11.1.3 *: Soit $q = p^n$. Tout sous-corps de $\mathbb{F}_q$ est de cardinal p^m, où m est un diviseur de n.*

En pratique il y a beaucoup de possibilités de construction de $\mathbb{F}_{p^m}$ comme un anneau quotient de type $\mathbb{F}_p[X]/(g(X))$, en choisissant un polynôme irréductible $g(X)$ de degré m.

Mais, si $q = p^n$, et m est un diviseur de n, alors $\mathbb{F}_{p^m}$ est le seul sous-corps de $\mathbb{F}_q$ d'ordre p^m, défini comme l'ensemble de toutes les racines du polynôme $X^{p^m} - X$ dans $\mathbb{F}_q$.

11.2 Polynômes sur les corps finis. Nombre de polynômes irréductibles de degré donné.

THÉORÈME 11.2.1 *: Soit p premier et q une puissance de p. Pour tout entier n strictement positif, il existe un polynôme P irréductible de degré n sur $\mathbb{F}_q$ et $\mathbb{F}_{q^n}$ est isomorphe à $\mathbb{F}_q[T]/(P)$.*

PREUVE. Soit θ un générateur du groupe cyclique $\mathbb{F}_{q^n}^*$. Alors $\mathbb{F}_{q^n} \cong \mathbb{F}_q[\theta]$. Soit P le polynôme minimale de θ sur $\mathbb{F}_q$. Alors P est un polynôme irréductible et $\mathbb{F}_{q^n}$ est un corps de rupture pour P. Autrement dit, on a un isomorphisme

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

qui envoie la classe de T sur θ. En particulier,

$$\deg P = \dim_{\mathbb{F}_q}(\mathbb{F}_q[T]/(P)) = \dim_{\mathbb{F}_q}(\mathbb{F}_{q^n}) = n.$$

REMARQUE 11.2.2 *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 $\mathbb{F}_{q^n}$.*

THÉORÈME 11.2.3 *: Soit 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 Q divise P.*

LEMME 11.2.4 *Soit P un polynôme irréductible sur $\mathbb{F}_q$ de degré m. Alors P divise $T^{q^n} - T$ si et seulement si m divise n.*

THÉORÈME 11.2.5 *: Soit P un polynôme irréductible sur $\mathbb{F}_q$ de degré m. Alors P possède une racine α dans $\mathbb{F}_{q^m}$. De plus, toutes les racines de P sont simples et sont données par α, $\alpha^q, \cdots, \alpha^{q^{m-1}}$, éléments distincts de $\mathbb{F}_{q^m}$.*

PREUVE. On a vu que $\mathbb{F}_{q^m}$ coïncide avec l'ensemble des racines du polynôme $T^{q^m} - T$ dans $\mathbb{F}_{q^m}$.

D'un autre coté, $T^{q^m} - T$ est divisible par P, puisque $T^{q^m} - T$ s'annule sur toute racine de P dans le corps $\mathbb{F}_q[T]/(P)$, de q^m éléments.

Ceci dit, parmi les racines de $T^{q^m} - T$ dans $\mathbb{F}_{q^m}$ se trouvent en particulier toutes les racines P, donc P possède une racine α dans $\mathbb{F}_{q^m}$.

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

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

où la dernière égalité vient du fait que $\mathrm{Fr}_q(x) = x$ pour tout $x \in \mathbb{F}_q$. Par conséquant $\alpha, \alpha^q, \cdots, \alpha^{q^{n-1}}$ sont des racines de P. Montrons par l'absurde que ces racines sont deux à deux distincts. En effet, dans le cas contraire, il existe i et j distincts avec $0 \leq i, j \leq n-1$ tels que $\alpha^{q^i} = \alpha^{q^j}$ et donc $\alpha^{q^i - q^j} = 1$. Quite à échanger i et j, on peut supposer $i > j$. Par conséquant

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

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

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

COROLLAIRE 11.2.6 *: Le corps de décomposition d'un polynôme P 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 polynôme irréductible unitaire $f = f_t$ de $\mathbb{F}_q[X]$ de degré d divisant n, alors

$$X^{q^n} - X = \prod_{d|n} \prod_{\substack{f \text{ unitaire} \\ \text{irréductible} \\ \deg f = d}} f(X),$$

PREUVE vient du fait que les ensembles des racines de la partie gauche et de la partie droite coïncident avec $\mathbb{F}_{q^n}$.

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.

DÉFINITION 11.2.7 *On appelle fonction de Moebius la fonction définie sur* $\mathbb{N}$ *par :*

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

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

THÉORÈME 11.2.8

(i) $X^{q^n} - X = \prod_{d|n} \prod_{\substack{f \text{ unitaire} \\ \text{irréductible} \\ \deg f = d}} f(X),$

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

La somme se faisant sur tous les diviseurs positifs de n.

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

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

La somme se faisant sur tous les diviseurs positifs de n.

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

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

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

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

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

Soient a_n, b_n deux suites de nombres liées par

$$b_n = \sum_{d|n} a_d$$

Alors

$$a_n = \sum_{d|n} \mu(n/d) b_d$$

(En effet

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

où $\delta = n/d|n/d'$. 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 $a_n = \sum_{d|n} \mu(n/d) b_d$ est facilement impliquée aussi par 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 cette formule montre que

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

On voit facilement (par l'absurde) que l'expression à droite est non nulle car elle est la somme des puissances différentes d'un nombre premier. D'autre part, $\nu_n \geq 0$; ceci implique $\nu_n > 0$, et on obtient de nouvau il existe un polynôme P irréductible de degré n sur $\mathbb{F}_q$.

Définition 11.2.9 *Soit P un polynôme sur $\mathbb{F}_q$ tel que $P(0) \neq 0$. L'ordre de P est le plus petit entier positif e tel que P divise $T^e - 1$. Si P(0)=0, alors il existe Q sur $\mathbb{F}_q$ non nul en 0 et h un entier positif tels que $P = T^h Q$, et dans ce cas on pose* $\mathrm{ord}(P) = \mathrm{ord}(Q)$.

Exercice. Montrer l'existence d'un tel nombre e.

Remarque 11.2.10 *Si P est irréductible de degré m sur $\mathbb{F}_q$, alors l'ordre de P divise $q^m - 1$.*

Théorème 11.2.11 *Le nombre de polynômes irréductibles unitaires sur $\mathbb{F}_q$ de degré m et d'ordre e est*

$$N_{q,m,e} = \varphi(e)/m \text{ si } e > 1.$$

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

Preuve (en exercice).

Exemple. 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.

$$X^{23} - 1 = X^{23} + 1 = (x+1) g_0(x) g_1(x) =$$
$$(x+1)\left(x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1\right)\left(x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1\right)$$

où

$$g_0(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1 = \prod_{i \in I}(x - \alpha^i), I = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$$
$$g_1(x) = x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1 = \prod_{j \in J}(x - \alpha^j), J = \{5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22\}$$

REMARQUE. L'ensemble

$$I = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$$

coïncide avec l'ensemble des résidues 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-résidues quadratiques modulo 23.

L'application de Frobenius $\alpha^k \mapsto \alpha^{2k}$ laisse I et J stable puisque $\left(\frac{2}{23}\right) = 1$, et l'application $\alpha^k \mapsto \alpha^{-k}$ échange les ensembles I et J puisque $\left(\frac{-1}{23}\right) = -1$, grâce à la loi de réciprocité quadratique de Gauss : pour les nombres premiers positifs impairs p, q on a

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

et

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

REMARQUE 11.2.12 *: Le degré de P irréductible sur $\mathbb{F}_q$ d'ordre e est l'ordre multiplicatif de q modulo e.*

En effet, on a $e|q^m - 1$, avec un m minimal. Par exemple, si $e = 23$, $q = 2$, alors ord(2) mod 23 = 11.

DÉFINITION 11.2.13 *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'un racinie primitif de $\mathbb{F}_{q^m}$ (un générateur du groupe cyclique $\mathbb{F}_{q^m}^*$).*

THÉORÈME 11.2.14 *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 $q^m - 1$.*

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

THÉORÈME 11.2.15 *Soit α un élément de $\mathbb{F}_{q^m}$, une extension de $\mathbb{F}_q$. Soit d le degré de δ sur $\mathbb{F}_q$ 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) Q polynôme sur $\mathbb{F}_q$ est tel que $Q(\alpha) = 0$ si et seulement si P divise Q.
(iii) Q polynôme irréductible unitaire sur $\mathbb{F}_q$ et tel que $Q(\alpha) = 0$ est tel que $P = Q$.
(iv) P divise $x^{q^d} - 1$ et $x^{q^m} - 1$.
(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.
(vi) Si $P(\alpha) = 0$, alors 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 $q^d - 1$ dans $\mathbb{F}_{q^m}^*$.

EXERCICES

11.1 Ecrire les tables d'addition et de multiplication des corps $\mathbb{F}_4$, $\mathbb{F}_8$ et $\mathbb{F}_9$.

11.2 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 ?

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

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

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

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

11.7 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'un racinie primitif de $\mathbb{F}_{q^m}$ (un générateur du groupe cyclique $\mathbb{F}_{q^m}^*$). Trouver le nombre des polynômes primitifs de degré m sur $\mathbb{F}_q$.

11.8 Soit p premier impair. Montrer que $\mathbb{F}_{p^2}$ est un corps de rupture de $X^4 + 1$ sur $\mathbb{F}_p$. Si $\alpha^4 + 1 = 0$ 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 $p \equiv \pm 1 \bmod 8$.

Cours N°10. Jeudi le 11 decembre 2003

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

THÉORÈME 11.2.15. *Soit α un élément de $\mathbb{F}_{q^m}^*$, une extension de $\mathbb{F}_q$. Soit d le degré de $\mathbb{F}_q(\alpha)$ sur $\mathbb{F}_q$ 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) Q polynôme sur $\mathbb{F}_q$ est tel que $Q(\alpha) = 0$ si et seulement si P divise Q.

(iii) Q polynôme irréductible unitaire sur $\mathbb{F}_q$ et tel que $Q(\alpha) = 0$ est tel que $P = Q$.

(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.

(vi) Si $P(\alpha) = 0$, alors 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 $q^d - 1$ dans $\mathbb{F}_{q^m}^*$.

Constructions d'isomorphismes à partir des polynômes irréducibles

On commence par un exemple de calcul en Maple.

```
> 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;
```

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

On voit bien que les polynômes $P = T^3 + 2T^2 + T + 1$ et $Q = T^3 + T^2 + 2T + 1$ sont irréductibles sur $\mathbb{F}_3$.

EXEMPLE 11.2.16 *Construire un isomorphisme entre $\mathbb{F}_3[T]/(P)$ 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 aussi a 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 $c_0, c_1, c_2 \in \mathbb{F}_3$ (en exercice obligatoire).

11.3 Théorème de la base normale

EXEMPLE 11.3.1 *Considérons le polynôme $p(x) = x^4 + x + 1$. Il est primitif sur $\mathbb{F}_2$ et une de ses racines α 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

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

sont toutes les racines de $p(x) = x^4 + x + 1$, On observe ces éléments sont linéairement dépendants.

Ceci dit, $\{1, \alpha, \alpha^2, \alpha^3\}$ est une base de $\mathbb{F}_{16}$ sur $\mathbb{F}_2$, mais $\{\alpha, \alpha^2, \alpha^4, \alpha^8\}$ n'est pas une base.

Cependant , on montrera le résultat suivant :

THÉORÈME 11.3.2 (DE LA BASE NORMALE) *Soit p un nombre premier et $q = p^d$. Alors il existe un élément θ de $\mathbb{F}_q$ de sorte que $(\theta, \mathrm{Fr}_p(\theta), \cdots, \mathrm{Fr}_{p^{d-1}}(\theta))$ forment 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 $T^q - T = 0$, on a que $\mathrm{Fr}_q = \mathrm{Id}_{\mathbb{F}_q}$, et donc $T^d - 1$ appartient au noyau $\mathfrak{a}$. Inversement, si $P = \sum_{i=0}^{m} a_i T^i$ appartient à ce noyau avec $m < d$, on a la relation

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

Mais on sait que les automorphismes Id, Fr_p, $\cdots$, Fr_p^{d-1} sont deux à deux distincts et linéairement indépendants, cela implique que P est nul. On a donc obtenu que $\mathfrak{a} = (T^d - 1)$.

La décomposition de $\mu = T^d - 1$ en produit de polynômes irréductibles de $\mathbb{F}_p[T]$ donne une décomosition de $\mathbb{F}_q$ 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 $\mathbb{F}_p$-sous-espace stable par Fr_p, et par l'indépendance linéaire des Fr_p^i, 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 $a_0, a_1, \cdots, a_{r_i - 1} \in \mathbb{F}_p$ on a

$$a_0\beta_i + a_1 P_i(\mathrm{Fr}_p)(\beta_i) + \cdots + a_{r_i-1} P_i^{r_i-1}(\mathrm{Fr}_p)(\beta_i) = 0$$
$$\Rightarrow a_0 P_i^{r_i-1}(\mathrm{Fr}_p)(\beta_i) + a_1 P_i^{r_i}(\mathrm{Fr}_p)(\beta_i) + \cdots + a_{r_i-1} P_i^{2r_i-1}(\mathrm{Fr}_p)(\beta_i) = 0$$
$$\Rightarrow a_0 = 0 \Rightarrow a_1 = 0 \cdots \Rightarrow a_{r_i-1} = 0,$$

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 $\mathbb{F}_q$. S'il existe des éléments $a_k \in \mathbb{F}_p$ tels que $\sum_{k=0}^{d-1} a_k \mathrm{Fr}_p^k(\theta) = 0$, 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 $1 \leq i \leq s$, donc par μ, et tous les a_k sont nuls. Cela signifie que l'élément θ engendre bien une base normale de $\mathbb{F}_q$ sur $\mathbb{F}_p$.

Remarque 11.3.3 *Pour les corps de caractéristique 2, les bases normales permettent de calculer les carrés et donc les puissances. En effet, si $(\theta, \theta^2, \cdots, \theta^{2^{d-1}})$ forment 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.*

Exercices

11.1 Ecrire les tables d'addition et de multiplication des corps $\mathbb{F}_4$, $\mathbb{F}_8$ et $\mathbb{F}_9$.

11.2 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 ?

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

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

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

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

11.7 Soit p premier impair. Montrer que $\mathbb{F}_{p^2}$ est un corps de rupture de $X^4 + 1$ sur $\mathbb{F}_p$. Si $\alpha^4 + 1 = 0$ 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 $p \equiv \pm 1 \bmod 8$.

11.8 Montrer que le degré d'un polynôme P irréductible sur $\mathbb{F}_q$ d'ordre e est l'ordre multiplicatif de q modulo e. (En effet, on a $e | q^m - 1$, avec un m minimal).

11.9 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'un racinie primitif de $\mathbb{F}_{q^m}$ (un générateur du groupe cyclique $\mathbb{F}_{q^m}^*$).
(a) Trouver le nombre des 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 $q^m - 1$.

12 Algorithme de factorisation de Berlekamp dans $A = \mathbb{F}_q[X]$

On va présenter une méthode classique de factorisation d'un polynôme $f \in \mathbb{F}_q[X]$ (la méthode de Berlekamp). On suppose que f n'a pas de facteurs multiples (sinon on trouve un diviseur non-trivial comme $\mathrm{pgcd}(f(X), f'(X))$. Soit $f = h_1 \cdot \cdots \cdot h_s$ une décomposition inconnue de f en produit de facteurs irréductibles non-associés. Soit $A = \mathbb{F}_q[X]$, et considérons l'anneau quotient

$$A/(f) \cong A/(h_1) \oplus \cdots \oplus A/(h_s),$$

où $A/(h_i)$ sont des corps finis de q^{d_i} éléments, $d_i = \deg h_i$, et on a utilisé le théorème chinois. C'est un espace vectoriel de dimension $d = \deg f$ sur $\mathbb{F}_q$, dans lequel l'endomorphisme de Frobenius $\mathrm{Fr}_q : x \mapsto x^q$

opère $\mathbb{F}_q$–linéairement. Soit $\mathcal{K}$ le corps de décomposition de f sur $\mathbb{F}_q$, alors tout $A/(h_i)$ est isomorphe à un sous-corps $\mathcal{K}_i \subset \mathcal{K}$ tel que $\mathcal{K}_i \supset \mathbb{F}_q$, $[\mathcal{K}_i : \mathbb{F}_q] = d_i$.

De plus $A/(h_i) \cong \mathcal{K}_i \cong \mathbb{F}_{q^{h_i}}$ est donnée par la condition :

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

et pour son sous–anneau des constantes on a $\mathbb{F}_q = \{x \in A/(h_i) \mid x^q = x\}$. Alors

$$\begin{aligned}&\mathrm{Ker}(\mathrm{Fr}_q - \mathrm{Id})|(A/(f))\\ &\cong \mathrm{Ker}(\mathrm{Fr}_q - \mathrm{Id})|(A/(h_1)) \oplus \cdots \oplus \mathrm{Ker}(\mathrm{Fr}_q - \mathrm{Id})|(A/(h_s)) \cong \mathbb{F}_q^s.\end{aligned}$$

où s est le nombre de polynômes irréductibles h_i.

On obtient le critère d'irréductibilité de f : f est irréductible si et seulement si le rang r de l'opérateur $\mathrm{Fr}_q - \mathrm{Id}$ est égal à $d - 1$.

THÉORÈME 12.0.1 (CRITÈRE D'IRRÉDUCTIBILITÉ) *Soit f un polynôme de degré d sur $\mathbb{F}_q$. Alors f est irréductible si et seulement si le rang de* $\mathrm{Fr}_q - \mathrm{Id}$ *dans l'espace*

$$A/(f) \cong A/(h_1) \oplus \cdots \oplus A/(h_s)$$

est égal à $d - 1$.

Pratiquement on trouve la matrice de $\mathrm{Fr}_q - \mathrm{Id}$ dans une base de $A/(f)$ par exemple, dans la base

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

Soit $r < d - 1$; pour trouver les facteurs h_i inconnus on prend tout d'abord un polynôme h tel que

$$h + (f) \in \mathrm{Ker}(\mathrm{Fr}_q - \mathrm{Id}) \subset A/(f)$$

et $h + (f)$ n'est pas une constante $\mathrm{mod} f$. C'est possible grâce au fait que

$$\dim(\mathrm{Im}(\mathrm{Fr}_q - \mathrm{Id})) = \mathrm{rk}(\mathrm{Fr}_q - \mathrm{Id}) = d - s < d - 1 \Rightarrow \dim(\mathrm{Ker}(\mathrm{Fr}_q - \mathrm{Id})) = d - \mathrm{rk}(\mathrm{Fr}_q - \mathrm{Id}) \geq 2.$$

Alors $f | h^q - h$ puisque $h + (f) \in A/(f) \in \mathrm{Ker}(\mathrm{Fr}_q - \mathrm{Id})$, et

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

mais $h - \alpha \not\equiv 0 \bmod f$. Ceci implique que

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

mais les facteurs à droite ne sont pas tous triviaux car $\mathrm{pgcd}(f, h - \alpha) \neq f$. On cherche h ("un polynôme décomposant") sous la forme $h(X) = a_1 X + a_2 X^2 + \cdots + a_{d-1} X^{d-1}$, et on trouve les coefficients a_i comme une solution non triviale du système des équations linéaires $\mathrm{Ker}(\mathrm{Fr}_q - \mathrm{Id})(h) = 0$ dans $A/(f)$.

Bases de la méthode de Berlekamp

(voir section **??**).

Cours N°11. Jeudi le 18 decembre 2003

13 Equations algébriques et variétés affines

13.1 Systèmes algébriques

Soit K un anneau commutatif. On considère un système algébrique sur K :

$$X : F_i(T_1, \cdots, T_n) = 0 \quad (i \in I) \text{ où } F_i(T_1, \cdots, T_n) \in K[T_1, \cdots, T_n].$$

L'ensemble des solutions de X dans K est

$$X(K) = \{(x_1, \cdots, x_n) \in K^n \mid \forall i, F_i(x_1, \cdots, x_n) = 0\},$$

Il se peut que $X(K) = \emptyset$, c'est à dire, que le système n'a pas de solutions dans K, mais il existe des solutions dans un autre anneau.

Soit L une $K-$ algèbre commutative, c'est à dire, un anneau muni de morphisme de structure $\gamma : K \to L$. Alors on obtient une multiplication externe d'éléments $x \in L$ par $a \in K$, donnée par la formule : $a \cdot x = \gamma(a)x \in L$. Par exemple, $\mathbb{C}$ est une $\mathbb{R}$-algèbre, et tout anneau B est une $\mathbb{Z}$-algèbre.

Alors pour tout $(x_1, \cdots, x_n) \in L^n$ on définie la valeur du polynôme $F_i(x_1, \cdots, x_n) \in L$, et on pose

$$X(L) = \{(x_1, \cdots, x_n) \in L^n \mid \forall i, F_i(x_1, \cdots, x_n) = 0\},$$

l'ensemble des solutions de X dans L.

En particulier, tout anneau B est une $\mathbb{Z}$-algébre, donc $X(B)$ est défini pour tout système algébrique sur $\mathbb{Z}$.

PROPOSITION 13.1.1 *Soit (P_X) l'idéal de $K[T_1, \cdots, T_n]$, engendré par les polynômes*

$$F_i(T_1, \cdots, T_n) \in K[T_1, \cdots, T_n](i \in I),$$

et on considère l'anneau quotient $A_X = K[T_1, \cdots, T_n]/(P_X)$.

(a) Il existe une bijection

$$X(L) \leftrightarrow \mathrm{Hom}_{K-alg}(A_X, L) \text{ tel que } \mathbf{x} = (x_1, \cdots, x_n) \in L^n \leftrightarrow (s_{\mathbf{x}} : T_j \mapsto x_j).$$

(b) Pour tout morphisme $f : L_1 \to L_2$ de K-algèbres, il existe une application canonique d'ensembles des solutions

$$f_X : X(L_1) \to X(L_2) \text{ tel que } f_X((x_1, \cdots, x_n)) = (f(x_1), \cdots, f(x_n))$$

PREUVE. (a) On vérifie que

$$s_{\mathbf{x}} : K[T_1, \cdots, T_n] \to L, \quad s_{\mathbf{x}} : T_j \mapsto x_j),$$

est bien défini sur l'anneau quotient $A_X = K[T_1, \cdots, T_n]/(P_X)$.

(b) On vérifie que la formule $f_X((x_1, \cdots, x_n)) = (f(x_1), \cdots, f(x_n))$ détérmine f_X de façon unique.

EXEMPLE 13.1.2 *Pour voir que $N = 4m + 3$ n'est pas une somme de deux carrés : prenons*

$$L_1 = \mathbb{Z}, L_2 = \mathbb{Z}/4\mathbb{Z}, \quad X : T_1^2 + T_2^2 - N = 0,$$

alors

$$X(L_2) = \emptyset \Rightarrow X(L_1) = \emptyset.$$

13.2 Variétés affines (préparation).

Soit K un corps algébiquement clos. Dans ce cas un système algébique X sur K est essentiellement déterminé par l'ensemble des solutions $X(K) \subset K^n$, selon un résultat important de l'algèbre commutative :

THÉORÈME 13.2.1 ("NULLSTELLENSATZ") (LE THÉORÈME DES ZÉROS DE HILBERT, SANS DÉMONSTRATION) *Soit K un corps algébiquement clos. Soit $(P_X) = (F_i)_{i\in I}$ l'idéal de $K[T_1, \cdots, T_n]$, engendré par les polynômes*

$$F_i(T_1, \cdots, T_n) \in K[T_1, \cdots, T_n] \quad (i \in I),$$

et on considère l'anneau quotient $A_X = K[T_1, \cdots, T_n]/(P_X)$. Alors

$$F \in K[T_1, \cdots, T_n] \text{ s'annulle sur } X(K) \Longleftrightarrow \exists N, F^N \in P_X = (F_i)_{i\in I}$$

REMARQUE 13.2.2 *Soit $(P_X) = (F_i)_{i\in I}$ l'idéal de $K[T_1, \cdots, T_n]$, engendré par les polynômes*

$$F_i(T_1, \cdots, T_n) \in K[T_1, \cdots, T_n] \quad (i \in I).$$

Alors la condition

$$\exists N, F^N \in P_X = (F_i)_{i\in I}$$

signifie qu'on a $\overline{F}^N = 0$ dans l'anneau quotient $A_X = K[T_1, \cdots, T_n]/(P_X)$, où $\overline{F} = F \bmod P_X$

DÉFINITION 13.2.3 *Soit K un corps algébiquement clos, Alors l'*ensemble des solutions *$X(K) \subset K^n$ d'un système algébrique sur K,*

$$X : F_i(T_1, \cdots, T_n) = 0 \quad (i \in I) \text{ où } F_i(T_1, \cdots, T_n) \in K[T_1, \cdots, T_n],$$

est dit une variété affine *sur K*

On peut supposer que l'anneau quotient $A_X = K[T_1, \cdots, T_n]/(P_X)$ n'a pas d'éléments nilpotents, où $(P_X) = (F_i)_{i\in I}$ l'idéal de $K[T_1, \cdots, T_n]$, engendré par les polynômes

$$F_i(T_1, \cdots, T_n) \in K[T_1, \cdots, T_n] \quad (i \in I).$$

13.3 Résolution d'un système linéaire dans un anneau euclidien

On considère un système linéaire sur un anneau euclidien $\mathcal{A}$:

$$Ax = b, \text{ où } A = \begin{pmatrix} a_{11} & \cdots & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & \cdots & \cdots & a_{mn} \end{pmatrix} \in M_{mn}(\mathcal{A}),$$

$$x = \begin{pmatrix} x_1 \\ \cdots \\ \cdots \\ x_n \end{pmatrix} \in M_{n1}(\mathcal{A}), b = \begin{pmatrix} b_1 \\ \cdots \\ \cdots \\ b_m \end{pmatrix} \in M_{m1}(\mathcal{A}).$$

Pour résoudre un tel système on a besoin de la théorie des diviseurs élémentaires. Rappellons qu'une transformation élémentaire de lignes d'une matrice sur un anneau commutatif $\mathcal{A}$ c'est l'addition à une ligne d'une autre, multipliée par un élément de $\mathcal{A}$. De façon similaire on définit les transformations élémentaires entières de colonnes. Une transformation élémentaire de lignes (resp. de colonnes) est équivalente à la multiplication à gauche (respectivement, à droite) de la matrice initiale par une matrice de type $E_{ij} = E + \lambda e_{ij}$ (avec $i \neq j$) dans le groupe $SL_m(\mathcal{A})$ (resp. $SL_n(\mathcal{A})$). Si l'on fait plusieures telles transformations à la suite, on remplace la matrice A par UAV où $U \in GL_m(\mathcal{A})$, $V \in GL_n(\mathcal{A})$ sont des matrices à coefficients entiers inversibles sur $\mathcal{A}$, c'est à dire, telles que $\det U, \det V \in \mathcal{A}^*$.

Définition 13.3.1 *On définit des* matrices élémentaires *$U \in \mathrm{GL}_m(\mathcal{A})$ et $V \in \mathrm{GL}_n(\mathcal{A})$ comme les matrices obtenues à partir des matrices unités I_m et I_n par une transformation éléméntaire des lignes (colonnes) sur $\mathcal{A}$.*

Remarque 13.3.2 *On vérifie que la matrice UAV est obtenue en appliquant aux lignes (colonnes) de A les mêmes transformations élémentaires qui ont été utilisé dans la définition de U et V ci-dessus.*

Proposition 13.3.3 *Pour toute matrice*

$$A = \begin{pmatrix} a_{11} & \cdots & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & \cdots & \cdots & a_{mn} \end{pmatrix} \in M_{mn}(\mathcal{A}),$$

on peut choisir des produits $U = U_1 \cdot U_2 \cdot \cdots \cdot U_k$ et $V = V_1 \cdot V_2 \cdot \cdots \cdot V_l$ des matrices élémentaires de telle façon que $UAV = D$, avec

$$D = \begin{pmatrix} d_1 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & d_2 & 0 & \cdots & \cdots & 0 \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & \cdots & \cdots & d_r & \cdots & 0 \\ 0 & \cdots & \cdots & \cdots & 0 & 0 \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 \end{pmatrix} \in M_{mn}(\mathcal{A}), \qquad \begin{array}{l} \text{où } r \text{ est le rang de } A, \\ \text{et } d_1, \cdots, d_r \neq 0 \\ \text{avec } d_1 | d_2 \cdots | d_r. \end{array}$$

Corollaire 13.3.4 *On en déduit que*

$$Ax = b \Longleftrightarrow UAVV^{-1}x = Ub \Longleftrightarrow Dy = c, \text{ où } c = Ub, y = V^{-1}x, x = Vy,$$

et s'il existe une solutions, alors la solution générale sur $\mathcal{A}$ est donnée par les formules

$$d_i y_i = c_i, \text{ pour } i \leq r, y_i \in \mathcal{A} \text{ pour } i > r, \begin{pmatrix} x_1 \\ \cdots \\ \cdots \\ \cdots \\ x_n \end{pmatrix} = V \begin{pmatrix} c_1/d_1 \\ \cdots \\ c_r/d_r \\ y_{r+1} \\ y_n \end{pmatrix}.$$

Calculs avec les matrices élargies

Pour trouver U et V on utilise les matrices élargies

$$\left(\begin{array}{c|c} A & b \\ \hline I_n & 0 \end{array}\right)$$

Montrer que par les transformations élémentaires de lignes et de colonnes la matrice élargie se transforme en

$$\left(\begin{array}{c|c} A & b \\ \hline I_n & 0 \end{array}\right) \sim \left(\begin{array}{c|c} UAV & Ub \\ \hline V & 0 \end{array}\right)$$

Exemple 13.3.5 *Résoudre les système linéaires sur $\mathbb{Z}$:*

(a)

$$5x_1 + 6x_2 + 7x_3 = 4.$$

(b)

$$\begin{cases} x_1 + x_2 + x_3 = 2 \\ 4x_1 + x_2 + 4x_3 = 5 \\ x_1 - 2x_2 + x_3 = -1. \end{cases}$$

SOLUTION. (a) Ecrivons les matrices correspondantes :

$$\begin{pmatrix} 5 & 6 & 7 & 4 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 5 & 1 & 2 & 4 \\ 1 & -1 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 4 \\ -1 & 6 & 1 & 0 \\ 1 & -5 & -2 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

d'où

$$V = \begin{pmatrix} -1 & 6 & 1 \\ 1 & -5 & -2 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} -1 & 6 & 1 \\ 1 & -5 & -2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 4 \\ y_2 \\ y_3 \end{pmatrix},$$

avec y_2, $y_3 \in \mathbb{Z}$.

SOLUTION. (b) Ecrivons les matrices correspondantes :

$$\begin{pmatrix} 1 & 1 & 1 & 2 \\ 4 & 1 & 4 & 5 \\ 1 & -2 & 1 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & 2 \\ 0 & -3 & 0 & -3 \\ 0 & -3 & 0 & -3 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & 3 & 0 & 3 \\ 0 & 0 & 0 & 0 \\ 1 & -1 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

d'où

$$V = \begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \\ y_3 \end{pmatrix},$$

avec $y_3 \in \mathbb{Z}$.

13.4 Systèmes diophantiens linéaires.

L'algorithme d'Euclide nous permet d'étudier un système diophantien linéaire (comme un cas particulier de section 13.3) :

$$Ax = b, \tag{13.1}$$

où

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \ddots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \in M_{m,n}(\mathbb{Z}), \quad x = \begin{pmatrix} x_1 \\ \cdots \\ x_n \end{pmatrix}, b = \begin{pmatrix} b_1 \\ \cdots \\ b_m \end{pmatrix}.$$

De l'autre cotê, le système

$$UAVy = Ub \tag{13.2}$$

est équivalent à (13.1) car ses solutions correspondent bijectivement aux solutions de (13.1) par : $x = Vy$. On utilise cette observation pour remplacer A par une matrice plus simple $A' = UAV$. En effet, si l'on utilise l'algorithme d'Euclide et une version de la procédure d'élimination de Gauss sans divisions, on trouve A' de la forme

$$D = \begin{pmatrix} d_1 & 0 & 0 & \dots & 0 \\ 0 & d_2 & 0 & \dots & 0 \\ \dots & \dots & \ddots & \dots & 0 \\ 0 & 0 & \dots & d_r & \dots \\ 0 & 0 & \cdots & \cdots & 0 \end{pmatrix} = UAV \quad (r = \mathrm{rk}A). \tag{13.3}$$

Alors on voit que soit notre système est non–résoluble même sur $\mathbb{Q}$, soit on obtient toutes les solutions des équations $d_i y_i = c_i, \quad c = Ub$ pour $i \leq r$, $0y_i = 0$ pour $i > r$. Il est donc clair que l'ensemble des solutions entières est non–vide si et seulement si d_i divise c_i pour $i \leq r$ et il est paramétré de façon évidente. Le nombre $d_1 \cdot \ldots \cdot d_i$ coïncide avec le pgcd de tous les mineurs d'ordre i de A donc on peut supposer que $d_i | d_{i+1}$. Ils sont appellés *les diviseurs élémentaires* de A.

Pour trouver la matrice $V \in GL_n(\mathbb{Z})$ il est commode d'utiliser la matrice élargie $\begin{pmatrix} A & b \\ E_n & 0 \end{pmatrix}$, et si l'on applique les transformations élémentaires de n premières colonnes et m premières lignes ci–dessus, on obtient

$$\begin{pmatrix} A' & b' \\ V & 0 \end{pmatrix} = \begin{pmatrix} UAV & Ub \\ V & 0 \end{pmatrix}.$$

PROPOSITION 13.4.1 *(a) Un système linéaire*

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \cdots\cdots\cdots\cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m. \end{cases} \tag{13.4}$$

sur $\mathbb{Z}$ est résoluble si et seulement si il est résoluble $\bmod N$ *pour tout nombre naturel positif N.*

(b) Un système linéaire

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \cdots\cdots\cdots\cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m. \end{cases}$$

sur $\mathbb{Z}$ est résoluble si et seulement si pour tout nombre naturel positif $k \leq m, n$ le PGCD de tous les mineurs d'ordre k de la matrice A est égal au PGCD de tous les mineurs d'ordre k de la matrice élargie $(A|b)$.

En effet, cette méthode montre que (13.4) est résoluble si et seulement si ses diviseurs élémentaires coïncident avec ceux de la matrice étendue (avec la colonne b ajoutée). C'est équivalent à la résolubilité de toutes les congruences

$$Ax \equiv b (\bmod N)$$

où N un entier (on le voit sous la forme diagonale). Cette condition peut être étendue pour un système général diophantien. Il est clair, qu'une telle condition est nécessaire pour l'existence d'une solution. Notre étude montre que cette condition est aussi suffisante pour un système linéaire. Quand c'est vrai pour une classe d'équations diophantiennes, on dit que pour cette classe le principe de Minkowski–Hasse est vérifié. Le problème de validité du principe de Minkowski–Hasse pour les classes d'équations diophantiennes est un des problèmes centraux en théorie des nombres.

Groupes abéliens

(a) Soit F un groupe abélien libre (additif) de base $\{e_1, \cdots, e_n\}$, $F \cong \mathbb{Z}^n$, et soit H son sous-groupe engendré par des éléménts

$$f_j = \sum_{j=1}^{n} a_{ij} e_i \quad (i = 1, \cdots, n).$$

Montrer que le groupe quotient F/H est fini si et seulement si $\det(a_{ij}) \neq 0$ et dans ce cas $\mathrm{Card}\,(F/H) = |\det(a_{ij})|$.

(b) Décomposer en somme directe de groupes cycliques le groupe quotient F/H d'un groupe abélien fini F de base (e_1, e_2, e_3), $F \cong \mathbb{Z}^3$, par son sous-groupe H engendré par des éléménts f_1, f_2, f_3, avec

$$\begin{cases} f_1 = 7e_1 + 2e_2 + 3e_3 \\ f_2 = 21e_1 + 8e_2 + 9e_3 \\ f_3 = 5e_1 - 4e_2 + 3e_3. \end{cases}$$

(c) Décomposer en somme directe de groupes cycliques le groupe quotient F/H d'un groupe abélien fini F d'une base (e_1, e_2, e_3), $F \cong \mathbb{Z}^3$, par son sous-groupe H engendré par des éléménts f_1, f_2, f_3, avec

$$\begin{cases} f_1 = 2e_1 + 3e_2 + 4e_3 \\ f_2 = 5e_1 + 5e_2 + 6e_3 \\ f_3 = 2e_1 + 6e_2 + 9e_3. \end{cases}$$

(d) Même question pour les éléménts f_1, f_2, f_3, avec

$$\begin{cases} f_1 = 4e_1 + 7e_2 + 3e_3 \\ f_2 = 2e_1 + 3e_2 + 2e_3 \\ f_3 = 6e_1 + 10e_2 + 5e_3. \end{cases}$$

Rappel : systèmes linéaires dans $\mathbb{F}_{p^d}$ (F.Sergeraert)

```
> restart :
```

- Exemple dans $\mathbb{F}_{3^4}$.

- On prend un polynôme irréductible de degré 4 dans $\mathbb{F}_3$, affecté à **irr34**.

```
> irr34 := op(1, select(has, Factor(x^81-x) mod 3, 4)) ;
```

$$irr34 := x^4 + 2\,x^3 + 2\,x^2 + x + 2$$

- Le polynôme irréductible obtenu par ce procédé n'est pas forcément le même d'une session à l'autre.

- On aliasse α à une racine de ce polynôme dans une extension de $\mathbb{F}_3$, de sorte que $\mathbb{F}_{3^4} = \mathbb{F}_3[\alpha]$.

```
> alias(alpha = RootOf(irr34) mod 3) ;
```

$$\alpha$$

- La procédure **rnd3** génére un entier modulo 3 pseudo-aléatoire.

```
> rnd3 := rand(0..2) :
> seq(rnd3(), i = 1..5) ;
```

$$0, 2, 0, 2, 1$$

- La procédure **rnd34** génère un élément pseudo-aléatoire de $\mathbb{F}_{3^4}$.

```
> rnd34 := () -> add(rnd3()*alpha^i, i=0..3) :
> seq(rnd34(), i = 1..5) ;
```

$$2 + 2\,\alpha + 2\,\alpha^2 + \alpha^3,\ 1 + \alpha,\ 2 + 2\,\alpha + \alpha^2,\ 2\,\alpha^2,\ \alpha^2$$

- La matrice A est une matrice 3x3 pseudo-aléatoire à coefficients dans $\mathbb{F}_{3^4}$.

```
> A := matrix(3, 3, rnd34) ;
```

$$A := \begin{bmatrix} 1 + 2\,\alpha^2 + 2\,\alpha^3 & 2 + 2\,\alpha + 2\,\alpha^3 & 2 + 2\,\alpha^2 + 2\,\alpha^3 \\ 2\,\alpha^2 & 2 + \alpha + \alpha^2 & 1 + \alpha^3 \\ 2 + 2\,\alpha + \alpha^3 & 1 + \alpha^2 & \alpha + 2\,\alpha^2 \end{bmatrix}$$

- Idem pour un vecteur second membre.

```
> b := vector(3, rnd34) ;
```

$$b := \left[\alpha^3,\ \alpha^3,\ 2 + 2\,\alpha^2\right]$$

- Linsolve(...) mod 3 permet de résoudre dans $\mathbb{F}_{3^4}$.

```
> x := Linsolve(A,b) mod 3 ;
```

$$x := \left[\alpha^3 + 2\,\alpha^2 + 2,\ \alpha + \alpha^2,\ 2\right]$$

- Vérification. Calcul de $A\,x - b$.

```
> zerov := evalm(A &* x - b) ;
```

$$\begin{aligned} zerov := \Big[&(1 + 2\,\alpha^2 + 2\,\alpha^3)\,(\alpha^3 + 2\,\alpha^2 + 2) + (2 + 2\,\alpha + 2\,\alpha^3)\,(\alpha + \alpha^2) + 4 + 4\,\alpha^2 + 3\,\alpha^3, \\ &2\,\alpha^2\,(\alpha^3 + 2\,\alpha^2 + 2) + (2 + \alpha + \alpha^2)\,(\alpha + \alpha^2) + \alpha^3 + 2, \\ &(2 + 2\,\alpha + \alpha^3)\,(\alpha^3 + 2\,\alpha^2 + 2) + (1 + \alpha^2)\,(\alpha + \alpha^2) + 2\,\alpha + 2\,\alpha^2 - 2\Big] \end{aligned}$$

- Les termes du vecteur obtenu ne sont pas « réduits » à leur forme canonique dans $\mathbb{F}_{3^4} = \mathbb{F}_3[\alpha]$. Pour obtenir la réduction, on utilise

```
> map(item -> Expand(item) mod 3, zerov) ;
```

$$[0,\ 0,\ 0]$$

Cours N°12. Jeudi le 8 janvier 2004

13.2 Rappel : variétés affines

Soit K un corps algébiquement clos. Nous avons déjà remarqué que dans ce cas un système algébique X sur K est essentiellement déterminé par l'ensemble des solutions $X(K) \subset K^n$, selon un résultat important de l'algèbre commutative :

THÉORÈME 13.2.1 ("NULLSTELLENSATZ", LE THÉORÈME DES ZÉROS DE HILBERT, SANS DÉMONSTRATION) *Soit K un corps algébiquement clos. Soit $P_X = (F_1, \cdots, F_m)$ l'idéal de $K[T_1, \cdots, T_n]$, engendré par les polynômes*

$$F_1(T_1, \cdots, T_n), \cdots, F_m(T_1, \cdots, T_n) \in K[T_1, \cdots, T_n].$$

Alors

$$F \in K[T_1, \cdots, T_n] \text{ s'annulle sur tout } X(K) \Longleftrightarrow \exists N, F^N \in P_X = (F_1, \cdots, F_m)$$

NOTATIONS.

(a) Pour tout K-algèbre L, et pour tout idéal $I \subset K[T_1, \cdots, T_n]$ on pose

$$V(I, L) = \{(x_1, \cdots, x_n) \in L^n \mid \forall F \in I, F(x_1, \cdots, x_n) = 0\},$$

le sous-ensemble algébrique dans L^n. Alors $X(L) = V(P_X, L)$.

(b) De plus, on appelle racine de l'idéal I, et on note $\sqrt{I}$, l'idéal $\left\{F \in K[T_1, \cdots, T_n] | \exists N, F^N \in I\right\}$. C'est un idéal de $K[T_1, \cdots, T_n]$, et on vérifie facilement que $X(L) = V(\sqrt{P_X}, L)$, et que $\sqrt{\sqrt{I}} = \sqrt{I}$.

(c) Pour tout sous-ensemble $X \subset L^n$ on défini l'idéal des polynômes annullés sur X, et on le note par

$$J = J(X) \subset K[T_1, \cdots, T_n].$$

Alors le théorème 13.2.1 signifie que si K est un corps algébiquement clos, $L = K$, alors

$$\sqrt{P_X} = J(X(K)).$$

REMARQUE 13.2.2. *Soit $P_X = (F_1, \cdots, F_m)$ l'idéal de $K[T_1, \cdots, T_n]$, engendré par les polynômes*

$$F_1(T_1, \cdots, T_n), \cdots, F_m(T_1, \cdots, T_n) \in K[T_1, \cdots, T_n].$$

Alors la condition

$$\exists N, F^N \in P_X = (F_1(T_1, \cdots, T_n), \cdots F_m(T_1, \cdots, T_n))$$

signifie qu'on a $\overline{F}^N = 0$ dans l'anneau quotient $A_X = K[T_1, \cdots, T_n]/P_X$, où $\overline{F} = F \bmod P_X$. De plus l'anneau quotient

$$K[T_1, \cdots, T_n]/\sqrt{P_X}$$

n'a pas d'éléments nilpotents.

DÉFINITION 13.2.3. *Soit K un corps, et L un corps algébiquement clos contenant K,*
(a) L'ensemble des solutions $X(L) \subset L^n$ d'un système algébrique sur K,

$$X : F_1(T_1, \cdots, T_n) = 0, \cdots, F_m(T_1, \cdots, T_n) = 0 \text{ où } F_i(T_1, \cdots, T_n) \in K[T_1, \cdots, T_n],$$

est dit une variété affine $V = V_X$ dans L^n définie sur K.

(b)L'ensemble des solutions $X(K) \subset K^n$ d'un système algébrique sur K,

$$X : F_1(T_1, \cdots, T_n) = 0, \cdots, F_m(T_1, \cdots, T_n) = 0 \text{ où } F_i(T_1, \cdots, T_n) \in K[T_1, \cdots, T_n],$$

est dit l'ensemble des points rationnels $X(K) = V_X(K)$ sur K.

On peut supposer que l'anneau quotient $A_X = K[T_1, \cdots, T_n]/(P_X)$ n'a pas d'éléments nilpotents, où $P_X = (F_1, \cdots, F_m)$ l'idéal de $K[T_1, \cdots, T_n]$, engendré par les polynômes

$$F_1(T_1, \cdots, T_n), \cdots, F_m(T_1, \cdots, T_n) \in K[T_1, \cdots, T_n].$$

13.5 Variétés algébriques (exemples)

Equations sur les corps finis : solution d'une équation affine sur $\mathbb{F}_q$

Soit $K = \mathbb{F}_{p^l}$. On considère une équation affine $F(X, Y) = 0$ sur $\mathbb{F}_{p^l}$, par exemple $X^3 + Y^3 = 1$ sur $\mathbb{F}_8$ ($p = 2, l = 3$). On représent les éléments de $K = \mathbb{F}_{p^l}$ sous la forme des nombres n vérifiant $0 \leq n < p^l$. En effet, étant donné un tel nombre n, on le transforme en un élément de K en utilisant l'écriture de n en base p : il existe des entiers uniques ("Chiffres" de n en base p) $m_0, \ldots, m_{d-1}$ vérifiant $0 \leq m_i < p$ et tels que

$$n = m_0 + m_1\, p + m_2\, p^2 + \cdots + m_{d-1}\, p^{d-1},$$

ce qui permet d'associer de manière unique à l'entier n, l'élément

$$\mu = \overline{m_0 + m_1 T + \cdots + m_{d-1} T^{d-1}}$$

de K, $\alpha = \overline{T} = T \bmod f$.

```
> restart;
> F:=(X,Y)->X^3+Y^3-1;
> p:=2;l:=3;
> %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
> (la procedure gf engendre un générateur alpha d'un corps fini F_{p^l})
> gf:= proc(p::nonnegint,l::nonnegint)
> local u,i,m, v;
> if ((p-2)^2+(l-2)^2=0) then
> alias(alpha = RootOf(x^2+x+1) mod 2);
> fi;
> if l=1 then
> alpha=1;
> else fi;
> u:=op(1, select(has, Factor(z^(p^l)-z) mod p, z^l)) ;
> alias(alpha = RootOf(u) mod p);
> return alpha,u;
> end proc:
```

$$F := (X, Y) \to X^3 + Y^3 - 1$$

$$p := 2$$

$$l := 3$$

```
> #%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
> %%%%%%
> Chiffres:= proc(  d::nonnegint,l::nonnegint,n::nonnegint )
> local i,m, v;
> v:=vector(l);
> m:=n;
> for i from 0 to l-1 do
> v[l-i]:=modp(m,d);m:=floor(m/d); od;
> return v;
> #gf(p,l):
> end proc:
> gf(p,l):
> #%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
> %%%%%%
> g:= proc( p::nonnegint,l::nonnegint,n::nonnegint )
> local h, v, i;
> v:=vector(l);
> for i from 1 to l do
> v:=evalm(Chiffres(p,l,n));h:=add(alpha^(l-j)*v[j],j=1..l);return h;
> od;end proc:
> gf(p,l):
> #%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
> %%
> points:= proc(  p::nonnegint,l::nonnegint,F::polynom )
> local n1,n2,n3, L,c,v,f1, f2;
> c:=0:
> L:=NULL:
> for n1 from 0 to p^l-1 do
> for n2 from 0 to p^l-1 do
> if Eval(F(X,Y,Z),{X=g(p,l,n1),Y=g(p,l,n2)}) mod p =0 then c:=c+1;
> L:= L,(‘ c‘=c,[g(p,l,n1),g(p,l,n2)]);fi; od; od;
> return(‘ L‘=L):end:
> points(p,l,F);
```

$$L = (\ c = 1,\ [0,\ 1],\ \ c = 2,\ [1,\ 0],\ \ c = 3,\ [\alpha,\ 1 + \alpha^2 + \alpha],\ \ c = 4,\ [1 + \alpha,\ \alpha^2],\ \ c = 5,$$
$$[\alpha^2,\ 1 + \alpha],\ \ c = 6,\ [\alpha^2 + 1,\ \alpha^2 + \alpha],\ \ c = 7,\ [\alpha^2 + \alpha,\ \alpha^2 + 1],\ \ c = 8,\ [1 + \alpha^2 + \alpha,\ \alpha])$$

Equations sur les corps finis : solution d'un système affine sur $\mathbb{F}_q$

Soit $K = \mathbb{F}_{p^l}$. On considère un système d'équations affines

$$\begin{cases} F_1(X, Y, Z) = 0 \\ F_2(X, Y, Z) = 0 \end{cases}$$

sur $\mathbb{F}_{p^l}$, par exemple

$$\begin{cases} X^3 + Y^3 + Z^5 = 0 \\ X + Y + 1 = 0 \end{cases}$$

sur $\mathbb{F}_8$ ($p = 2, l = 3$). On représent les éléments de $K = \mathbb{F}_{p^l}$ sous la forme des nombres n vérifiant $0 \leq n < p^l$. En effet, étant donné un tel nombre n, on le transforme en un élément de K en utilisant l'écriture de n en base p : il existe des entiers uniques ("Chiffres" de n en base p) $m_0, \ldots, m_{d-1}$ vérifiant $0 \leq m_i < p$ et tels que

$$n = m_0 + m_1\, p + m_2\, p^2 + \cdots + m_{d-1}\, p^{d-1},$$

ce qui permet d'associer de manière unique à l'entier n, l'élément

$$\mu = \overline{m_0 + m_1 T + \cdots + m_{d-1} T^{d-1}}$$

de K, $\alpha = \overline{T} = T \bmod f$.

```
> restart;
> F1:=(X,Y,Z)->X^3+Y^3+Z^5;
> F2:=(X,Y,Z)->X+Y+1;
> p:=2;l:=3;
> %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% %%%%%%%
```

(la procedure gf engendre un générateur alpha d'un corps fini F_{p^l})

```
> gf:= proc(p::nonnegint,l::nonnegint)
> local u,i,m, v;
> if ((p-2)^2+(l-2)^2=0) then
> alias(alpha = RootOf(x^2+x+1) mod 2);
> fi;
> if l=1 then
> alpha=1;
> else fi;
> u:=op(1, select(has, Factor(z^(p^l)-z) mod p, z^l)) ;
> alias(alpha = RootOf(u) mod p);
> return alpha,u;
> end proc:
```

$$F1 := (X, Y, Z) \to X^3 + Y^3 + Z^5$$

$$F2 := (X, Y, Z) \to X + Y + 1$$

$$p := 2$$

$$l := 3$$

```
> Chiffres:= proc(  d::nonnegint,l::nonnegint,n::nonnegint )
> local i,m, v;
> v:=vector(l);
> m:=n;
> for i from 0 to l-1 do
> v[l-i]:=modp(m,d);m:=floor(m/d); od;
> return v;
> #gf(p,l):
> end proc:
> gf(p,l):
> g:= proc( p::nonnegint,l::nonnegint,n::nonnegint )
> local h, v, i, n3;
> v:=vector(l);
> for i from 1 to l do
> v:=evalm(Chiffres(p,l,n));h:=add(alpha^(l-j)*v[j],j=1..l);return h;
> #gf(p,l):
> od;end proc:
> gf(p,l):
> points:= proc(  p::nonnegint,l::nonnegint,F::polynom )
> local n1,n2,n3, L,c,v,f1, f2;
> c:=0:
> L:=NULL:
> for n1 from 0 to p^l-1 do
> for n2 from 0 to p^l-1 do
> for n3 from 0 to p^l-1 do
> if (Eval(F1(X,Y,Y),{X=g(p,l,n1),Y=g(p,l,n2),Z=g(p,l,n3)}) mod p=0
> and Eval(F2(X,Y,Z),{X=g(p,l,n1),Y=g(p,l,n2),Z=g(p,l,n3)}) mod p=0)
> then c:=c+1;
> L:= L,(` c`=c,[g(p,l,n1),g(p,l,n2),g(p,l,n3)]);fi; od; od;
> od;return(gf(p,l),` L`=L):end:
```

```
> points(p,l,F);
```

$$\alpha,\ z^3+z+1,\ L=(\ c=1,\ [0,\ 1,\ 0],\ \ c=2,\ [0,\ 1,\ 1],\ \ c=3,\ [0,\ 1,\ \alpha],\ \ c=4,\ [0,\ 1,\ 1+\alpha],$$
$$c=5,\ [0,\ 1,\ \alpha^2],\ \ c=6,\ [0,\ 1,\ 1+\alpha^2],\ \ c=7,\ [0,\ 1,\ \alpha^2+\alpha],\ \ c=8,\ [0,\ 1,\ 1],$$
$$c=9,\ [1+\alpha,\ \alpha,\ 0],\ \ c=10,\ [1+\alpha,\ \alpha,\ 1],\ \ c=11,\ [1+\alpha,\ \alpha,\ \alpha],\ \ c=12,$$
$$[1+\alpha,\ \alpha,\ 1+\alpha],\ \ c=13,\ [1+\alpha,\ \alpha,\ \alpha^2],\ \ c=14,\ [1+\alpha,\ \alpha,\ 1+\alpha^2],\ \ c=15,$$
$$[1+\alpha,\ \alpha,\ \alpha^2+\alpha],\ \ c=16,\ [1+\alpha,\ \alpha,\ 1],\ \ c=17,\ [1+\alpha^2,\ \alpha^2,\ 0],\ \ c=18,$$
$$[1+\alpha^2,\ \alpha^2,\ 1],\ \ c=19,\ [1+\alpha^2,\ \alpha^2,\ \alpha],\ \ c=20,\ [1+\alpha^2,\ \alpha^2,\ 1+\alpha],\ \ c=21,$$
$$[1+\alpha^2,\ \alpha^2,\ \alpha^2],\ \ c=22,\ [1+\alpha^2,\ \alpha^2,\ 1+\alpha^2],\ \ c=23,\ [1+\alpha^2,\ \alpha^2,\ \alpha^2+\alpha],\ \ c=24,$$
$$[1+\alpha^2,\ \alpha^2,\ 1],\ \ c=25,\ [1,\ \alpha^2+\alpha,\ 0],\ \ c=26,\ [1,\ \alpha^2+\alpha,\ 1],\ \ c=27,$$
$$[1,\ \alpha^2+\alpha,\ \alpha],\ \ c=28,\ [1,\ \alpha^2+\alpha,\ 1+\alpha],\ \ c=29,\ [1,\ \alpha^2+\alpha,\ \alpha^2],\ \ c=30,$$
$$[1,\ \alpha^2+\alpha,\ 1+\alpha^2],\ \ c=31,\ [1,\ \alpha^2+\alpha,\ \alpha^2+\alpha],\ \ c=32,\ [1,\ \alpha^2+\alpha,\ 1])$$
$$1:=1+\alpha^2+\alpha$$

Equations de degré deux

On considère l'équation diophantienne suivante aux coefficients entiers :

$$f(x_1,x_2,\ldots,x_n)=\sum_{i,j}^{n}a_{ij}x_ix_j+\sum_{i=1}^{n}b_ix_i+c=0. \tag{13.1}$$

Ici on commence par trouver l'ensemble de toutes les solutions en nombres rationnels. Ce problème est plus facile que ce de trouver les solutions en nombres entiers, mais il n'est pas trivial.

Un exemple classique est donné par la parametrisation rationnelle du cercle $x^2+y^2=1$:

$$x=\frac{2t}{1+t^2},\ \ y=\frac{1-t^2}{1+t^2},\quad (x=\cos\varphi,\ \ y=\sin\varphi,\ \ t=\tan\left(\frac{\varphi}{2}\right)), \tag{13.2}$$

$$(\text{ à l'exception du point } (0,-1)). \tag{13.3}$$

Cette parametrisation nous permet de décrire toutes les triples primitifs de Pythagore (X,Y,Z), c'est à dire, les solutions en entiers naturels de l'équation $X^2+Y^2=Z^2$ avec pgcd($X,\ Y,\ Z$) $=1$. La réponse est : $X=2uv,\ \ Y=u^2-v^2,\ \ Z=u^2+v^2$, où $u>v>0$ sont des entiers premiers entre eux. Pour le prouver, il suffit de poser $t=u/v$ dans (13.2).

De façon similaire, trouver les solutions rationnelles de (13.1) est equivalent à trouver les solutions rationnelles de l'équation homogène

$$\begin{aligned}F(X_0,X_1,\cdots,X_n)&=\sum_{i,j=0}^{n}f_{ij}X_iX_j\\&=\sum_{i,j=1}^{n}f_{ij}X_iX_j+2\sum_{i,j=1}^{n}f_{i0}X_iX_0+f_{00}X_0^2\end{aligned} \tag{13.4}$$

où $f_{ij}=f_{ji}=a_{ij}/2$ pour $1\le i<j\le n$ et $f_{0i}=f_{i0}=b_i/2$ pour $i=1,2,\ldots,n,\ \ f_{00}=c$. Les *coordonnées non–homogènes* $x_1,\cdots,x_n$ sont reliées aux *coordonnées homogènes* $X_0,\ldots,X_n$ par $X_i=x_iX_0\quad(i=1,2,\ldots,n)$. La forme quadratique $F(X)$ peut être écrit de façon commode sous la forme

$$F(X)=X^tA_FX,\quad X^t=(X_0,X_1,\ldots,X_n),$$

où $A_F = (f_{ij})$ est la matrice des coefficients. S'il existe une solution rationnelle non–triviale de $F(X) = 0$, on dit que la forme F *représente zéro sur* $\mathbb{Z}$.

Cette équation définie une conique Q_F (c'est à dire, une hypersurface de $\mathbb{CP}^n$ de degré deux). Ses points sont toutes les solutions (à l'exception de la solution triviale) considérées comme points de l'espace projectif complexe $\mathbb{CP}^n$:

$$Q_F = \{(z_0 : z_1 : \ldots : z_n) \in \mathbb{CP}^n \quad | \quad F(z_0, z_1, \ldots, z_n) = 0\}.$$

Toute solution non–triviale de $F(X) = 0$ donne un point sur cette conique. S'il on connait une solution X^0 alors on peut trouver toutes les autres en considérant les intersections deQ_F avec les droites (projectifs) defines sur $\mathbb{Q}$ et contenants X^0. Algébriqument, une droite passant par X^0 et Y^0 est formée par tous les points de la forme $uX^0 + vY^0$. L'équation $F(uX^0 + vY^0) = 0$ se réduit alors à

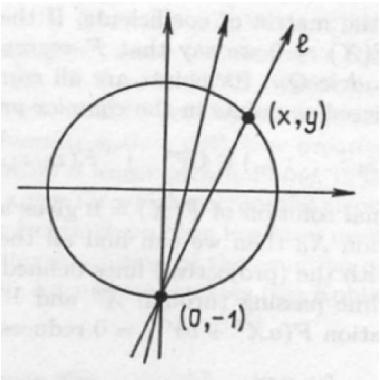
$$uv \sum_{i=1}^{n} \frac{\partial F}{\partial X_i}(X^0)Y_i^0 + v^2 F(Y^0) = 0.$$

En général, toutes les dérivées partielles $\dfrac{\partial F}{\partial X_i}$ne s'annulent pas nécessairement. Dans ce cas, pour tout Y^0 on peut trouver un point d'intersection de Q_F avec notre droite :

$$v = -u \sum_{i=1}^{n} \frac{\partial F}{\partial X_i}(X^0)Y_i^0 / F(Y^0). \tag{13.5}$$

(Si, par hasard, $F(Y^0) = 0$ alors Y^0 se trouve déjà sur Q_F). De nouveau, ce point n'est pas unique en général. Les cas limits peut être bien compris en termes géométriques : si toutes les dérivées partielles s'annulent en X^0 alors notre conique est un cône de sommet X^0, et le problème se réduit à ce de trouver tous les points rationnels sur la base d'un cône, cette base étant une conique de dimension inférieure ; s'il arrive qu'ils tous se trouvent entièrement sur Q_F alors tous ces points rationnels doivent être considérés etc.

Cette *méthode de la projection stereographique*, appliquée à $x^2 + y^2 = 1$ et au point (0,-1) donne exactement (13.2) s'il on note t la pente de la droite passant par (0,-1) et (x, y) : $\quad y + 1 = tx$.



Concernant l'équation

$$F(X_0, X_1, \ldots, X_n) = 0 \tag{13.6}$$

(avec F comme dans (13.4)) sur les nombres rationnels, on peut commencer par la diagonalisation de A_F avec une substitution linéaire non–dégénérée $X = CY$ où $C \in \mathrm{M}_{n+1}(\mathbb{Q})$. La matrice C peut être trovée effectivement par le méthode classique de l'extraction successive des carrées.

Pour les équations homogènes comme (13.6) les problèmes de trouver toutes les solutions dans $\mathbb{Q}$ et dans $\mathbb{Z}$ sont essentiellement équivalents. Lorsque on peut trouver toutes les solutions à partir d'une seule, la question-clé est donc de décider, s'il existe une solution. La réponse est donnée par le résuiltat suivante.

13.6 Le principe de Minkowski–Hasse pour les formes quadratiques

DÉFINITION 13.6.1 *Une solution* $(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$ *d'une equation* $F(x_1, x_2, \ldots, x_n) = 0$ *en nombres entiers est dit primitive modulo* N, *si* $\text{pgcd}(N, x_1, x_2, \ldots, x_n) = 1$.

THÉORÈME 13.6.2 *Une forme quadratique* $F(x_1, x_2, \ldots, x_n)$ *de rang* n *de coefficients entiers représente un zéro sur les nombres rationnels si et seulement si pour tout* N, *la congruence* $F(x_1, \ldots, x_n) \equiv 0 \pmod{N}$ *admet une solution primitive, et de plus* F *représents un zéro sur les nombres réels, c'est à dire, elle est indéfinie.*

Pour une preuve générale, voire [BS85]. Bien-sûr, la nécessité de cette condition est clair.

On donne ici une jolie démonstration de la suffisance de cette condition dans le cas $n = 3$ dûe à Legendre ([BS85]). Soit

$$F = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 \qquad (a_1a_2a_3 \neq 0).$$

Puisque F est indéfinie, on peut supposer que les deux premiers coefficients soient positifs, tandis que le troisième soit négatif. De plus, on peut les supposer sans facteurs carrés et premiers entre eux : on obtient ceci par des changements de variables et en divisant la forme par le pgcd de ses coefficients. On va noter une forme avec telles propriétés par

$$ax^2 + by^2 - cz^2. \tag{13.7}$$

Considérons un nombre premier p divisant c. Puisque $F \equiv 0 (\text{mod } p)$ admet une solution primitive, on peut trouver une solution non-primitive (x_0, y_0) de la congruence $ax^2 + by^2 \equiv 0 (\text{mod } p)$. Alors

$$ax^2 + by^2 \equiv ay_0^{-2}(xy_0 + yx_0)(xy_0 - yx_0) \pmod{p}.$$

Dans le cas $p = 2$ on a bien sûr

$$ax^2 + by^2 - cz^2 \equiv (ax + by - cz)^2 \pmod{2}.$$

Donc pour tout $p|2abc$ on peut trouver des formes linéaires $L^{(p)}$, $M^{(p)}$ en x, y, z de coefficients entiers telles que $F \equiv L^{(p)}M^{(p)} (\text{mod } p)$. En utilisant le théorème chinois , on trouve L (resp. M) de coefficients entiers congrue à $L^{(p)}$ (resp. $M^{(p)}$) (mod p) pour tout $p|abc$. On obtient donc

$$ax^2 + by^2 + cz^2 \equiv L(x, y, z)M(x, y, z) \pmod{abc}. \tag{13.8}$$

Considérons maintenant les point entiers dans la boîte suivante :

$$0 \leq x < \sqrt{bc}, \quad 0 \leq y < \sqrt{ac}, \quad 0 \leq z < \sqrt{ab}. \tag{13.9}$$

Si l'on exclut le cas trivial $a = b = c = 1$, on constate les racines carrées dans les inégalités (13.9) ne sont pas toutes de nombres entiers, donc le nombre total des points entiers sera strictement plus grand que le volume de cette boîte, i.e. abc. Ceci implique qu'il existe deux points différents pour lesquels L prends la même valeur mod abc. En considérant leurs différence, on trouve

$$L(x_0, y_0, z_0) \equiv 0 \pmod{abc} \tag{13.10}$$

pour un point $|x_0| \leq \sqrt{bc}, \quad |y_0| \leq \sqrt{ac}, \quad |z_0| \leq \sqrt{ab}$. Donc

$$ax_0^2 + by_0^2 - cz_0^2 \equiv 0 \pmod{abc} \tag{13.11}$$

et

$$-abc < ax_0^2 + by_0^2 - cz_0^2 < 2abc.$$

Il vient que soit

$$ax_0^2 + by_0^2 - cz_0^2 = 0 \tag{13.12}$$

soit

$$ax_0^2 + by_0^2 - cz_0^2 = abc. \tag{13.13}$$

Dans le premier cas le théorème est démontré. Dans le second cas on obtient explicitement la solution suivante :

$$a(x_0z_0 + by_0)^2 + b(y_0z_0 - ax_0)^2 - c(z_0^2 + ab)^2 = 0.$$

L'énoncé originale de Legendre a été que $ax^2 + by^2 - cz^2 = 0$ est résoluble si et seulement si toutes les classes résiduelles $bc \pmod a$, $\quad ac \pmod b$, $\quad -ab \pmod c$ sont des carrés.

On peut démontrer qu'une forme quadratique indefinite de rang ≥ 5 représente toujours un zéro sur les rationnels, voire [BS85].

13.7 Espace projectif $\mathbb{P}^n$, variétés algébriques

Soit K un corps et $n \geq 1$ un entier. On considère espace projectif de dimension n sur K et on note $\mathbb{P}^n_K$ ou simplement $\mathbb{P}^n$ l'ensemble des classes d'équivalence de $(n+1)$-uplets $(x_0, \cdots, x_n)$, $x_i \in F$ pour $0 \leq i \leq n$; sous la relation $(x_0, \cdots, x_n) \sim (\lambda x_0, \cdots, \lambda x_n)$ pour tout $\lambda \in K^*$. Une classe d'équivalence x est un point de $\mathbb{P}^n$. Soit $F[T] = F[T_0, \cdots, T_n]$. On interprète les éléments de $F[T]$ comme des fonctions régulières de l'espace affine $\mathbb{A}^{n+1}$, et on interprète les éléments de

$$F\left(\frac{T_1}{T_0}, \frac{T_2}{T_0}, \cdots, \frac{T_n}{T_0}\right),$$

comme des fonctions rationnelles de $\mathbb{P}^n$

Définition 13.7.3 *Une partie $X \subset \mathbb{P}^n$ est dit une variété algébrique projective si*

$$X = V(P) = \{x \in \mathbb{P}^n \mid \forall F \in P, F(x) = 0\}$$

où P est un idéal premier homogène de $F[T_0, \cdots, T_n]$, c'est à dire premier engendré par des polynômes homogènes.

Définition 13.7.4 *Soit U un voisinage ouvert d'un point x d'une variété projective X. Une application $f : U \to F$ est une fonction régulière au point x s'ils existent $F, G \in F[T_0, \cdots, T_n]$ des polynômes homogènes de même degré tels que $G(x) \in 0$ et $f = F/G$ dans un voisinage de x ; f est régulière sur U si elle est régulière en tout x de U.*

Définition 13.7.5 *Soit X une variété projective. L'idéal de X est l'ensemble*

$$I(X) = \{F \in F[T_0, \cdots, T_n] | F(x) = 0, \forall x \in X\}.$$

On définit également le corps des fonctions $K(X)$ de X comme le corps des fractions de la K-algèbre de type fini $K[T]/I(X)$.

Soit x un point de X et soient les couples (U, f) dans lesquels f est régulière sur U voisinage ouvert de x. On définit la relation d'équivalence suivante :

$$(U, f) \sim (U', f') \Longleftrightarrow f = f' \text{ sur } U \cap U'$$

dont les classes d'équivalences forment un anneau.

Cours N°13. Jeudi le 15 janvier 2004

14 Courbes planes.

14.1 Courbes planes affines.

Une courbe algébrique plane sur un corps K est formée par les points

$$\mathcal{C} : \{(x, y) \in K^2 \mid f(x, y) = 0\}$$

pour un polynôme non-constant $f(x, y)$ dans l'anneaux factoriel $K[x, y]$, donc $f = f_1^{k_1} \cdot \ldots \cdot f_r^{k_r}$, où f_i sont irréductibles non-proportionnels. Ceci implique que

$$\mathcal{C} = \cup_{i=1}^{r} \mathcal{C}_i,$$

où $\mathcal{C}_i : f_i = 0$ est une courbe dite irréductible.

Remarque 14.1.1

(a) Si K est algébriquement clos, alors $\mathcal{C} = \mathcal{C}(K)$ est infinie

(b) Si K est algébriquement clos, alors un polynôme g de $K[x, y]$ s'annule sur toute la courbe irréductible $\mathcal{C}_i(K)$ si et seulement si $f_i | g$.

14.2 Courbes planes projectives.

Rappelons qu'un point P du plan projectif $\mathbb{P}^2 = \mathbb{P}^2_K$ est donnée comme la classe d'équivalence, notée $(X : Y : Z)$, d'un triplet non-nul $(X, Y, Z) \in K^3 \backslash \{(0, 0, 0)\}$, de telle façon que $(X, Y, Z) \sim (X', Y', Z') = (\lambda X, \lambda Y, \lambda Z)$ $(\lambda \in K^*)$.

On a l'inclusion

$$\mathbb{A}^2 \hookrightarrow \mathbb{P}^2, \quad (x, y) \mapsto (x, y, 1),$$

qui donne tous les points de $\mathbb{P}^2$ avec $Z \neq 0$.

On a les relations suivantes entre les coordonnées affines (x, y) est les coordonnées projrctives $(X : Y : Z)$:

$$X = xZ, Y = yZ, \quad x = \frac{X}{Z}, y = \frac{Y}{Z}$$

Cartes affines

On a les trois parties suivantes de $\mathbb{P}^2$:

$$\mathbb{A}^2_1, \mathbb{A}^2_2, \mathbb{A}^2_3 \subset \mathbb{P}^2, \text{ telles que } \mathbb{A}^2_1 : X \neq 0, \ \mathbb{A}^2_2 : Y \neq 0, \ \mathbb{A}^2_3 : Z \neq 0.$$

isomorphes a K^2, et on a les coordonnées

$$\text{sur } \mathbb{A}^2_1 : X = xZ, Y = yZ, \quad x = \frac{X}{Z}, y = \frac{Y}{Z}$$
$$\text{sur } \mathbb{A}^2_2 : X = x'Y, Z = y'Y, \quad x' = \frac{X}{Y}, y' = \frac{Z}{Y}$$
$$\text{sur } \mathbb{A}^2_3 : Y = x''X, Z = y''X, \quad x'' = \frac{Y}{X}, y'' = \frac{Z}{X}$$

Exercice. Réécrire l'équation de la courbe de Fermat en coordonnées (x', y') et en (x'', y'').

Une courbe algébrique dans $\mathbb{P}^2$ est donnée par une équation homogène dans les coordonnées projectives : $F(X, Y, Z) = 0$, alors l'égalité $F(X, Y, Z) = 0$ ne dépend pas de choix des coordonnées projectives : si $(X', Y', Z') = (\lambda X, \lambda Y, \lambda Z)$, alors $F(X', Y', Z') = \lambda^d F(X, Y, Z) = 0$, où d est le degré homogène du polynôme F.

14.3 Points singuliers.

Soit K un corps. Rappelons qu'une courbe projective plane $\mathcal{C}$ sur K est définit par une équation de type $F(X:Y:Z)=0$, où $F(X:Y:Z)\in K[X,Y,Z]$ est une forme homogène des variables projectives X, Y, Z.

L'équation de la tangente dans les coordonnées affines a la forme

$$f'_x(P)(x-\alpha)+f'_y(P)(y-\beta)=0.$$

Par la construction,

$$f(x,y)=F(x,y,1),\ \text{où } F(X,Y,Z)=0 \text{ l'équation homogène de la courbe.}$$

Ceci implique : $f'_x=F'_x, f'_y=F'_y$, et selon le théorème connu de Euler (sur les fonctions homogènes) on a

$$XF'_X+YF'_Y+ZF'_Z=nF \text{ où } n \text{ est le degré de } F$$

Lorsque $P=(\alpha:\beta:1)$ se trouve sur la courbe alors

$$\alpha F'_X(P)+\beta F'_Y(P)+F'_Z(P)=nF,$$

donc l'équation de la tangente se transforme vers

$$xF'_X(P)+yF'_Y(P)+F'_Z(P)=0 \Longleftrightarrow XF'_X+YF'_Y+ZF'_Z=0.$$

Définition 14.3.1

(a) Un point singulier *sur une courbe projective plane $\mathcal{C}$ sur K est toute solution du système*

$$F=F'_X=F'_Y=F'_Z=0$$

dans une extension de K.

(b) On dit qu'une courbe projective plane $\mathcal{C}$ sur K est lisse *si le système*

$$F=F'_X=F'_Y=F'_Z=0$$

n'a pas de solutions non–triviales dans toute extension de K.

Exemple.

(a) Soit $Q(X,Y,Z)$ une forme quadratique de matrice A_Q, sur un corps K de caractéristique $\mathrm{Car}(K)\neq 0$. Montrer que la conique $Q(X,Y,Z)=0$ est non-singulière si et seulement si A_Q est inversible.

(b) Soit $Car(K)\neq 2,3$, et soit $\mathcal{C}$ donnée par l'équation homogène correspondante

$$Y^2Z=X^3+aXZ^2+bZ^3,\ O=(0:1:0).$$

On vérifie que cette courbe est lisse si et seulement si le polynôme cubique x^3+ax+b n'a pas de racines multiplies (directement par la définiton des points singuliers comme des solutions de l'équation $F=F'_X=F'_Y=F'_Z=0$ dans le cas général $F(X,Y,Z)=Y^2+a_1XYZ+a_3YZ^2-X^3-a_2X^2Z-a_4XZ^2-a_6Z^3$).

(c) Soit $K=\mathbb{F}_2$, et soit $\mathcal{C}$ une courbe sur K donnée par l'équation affine

$$y^2+y=x^3+ax+b,\ a,b\in\mathbb{F}_2$$

Montrer que cette courbe est toujours lisse (on n'a plus besoin d'exclure ici le cas des racines multiples).

(d) Soit $K=\mathbb{F}_3$, et soit $\mathcal{C}$ une courbe sur K donnée par l'équation affine :

$$y^2=x^3+ax^2+bx+c,\ a,b,c\in\mathbb{F}_3$$

Montrer que cette courbe est lisse si et seulement si le polynôme cubique à droite n'a pas de racines multiples.

14.4 Equations cubiques

Le problème de l'existence d'une solution.

Pour les *formes cubiques* $F(X, Y, Z)$ en trois variables de coefficients entiers, on ne connait pas d'algorithme qui decide en générale si l'équation $F = 0$ possède une solution non-triviale en nombres entiers. Grandes classes de telles equations ont étés étudiées de point de vue théorique et numerique ; par exemple Selmer E.S. en 1951–1954 a étudié en detail les équations de type

$$aX^3 + bY^3 + cZ^3 = 0.$$

Il arrive que même pour des équations simple comme $3X^3 + 4Y^3 + 5Z^3 = 0$ le principe de Minkowski–Hasse n'est pas valable : on peut montrer que cette équation n'a pas de solutions en nombres entiers, quoiqu'il existe des solutions réelles et des solution primitives modulo tout $N > 1$.

Addition de points sur une cubique plane

Toute forme cubique non-nulle $F(X,Y,Z)$ à coefficients entiers definie une courbe cubique $\mathcal{C}$ dans l'espace projectif $\mathbb{P}^2$ (sur $\mathbb{Q}$ et sur $\mathbb{C}$) :

$$\mathcal{C} = \{(X : Y : Z) \mid F(X, Y, Z) = 0\}. \tag{14.1}$$

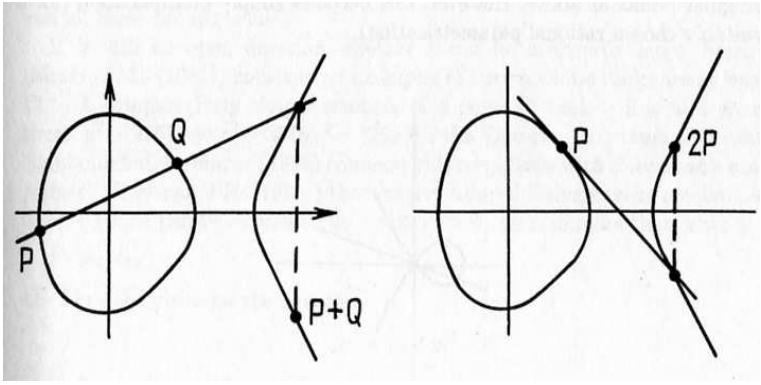
Si $\mathcal{C}$ est non-singulière et si $F = 0$ possède au moins une solution rationnelle, alors on peut trouver un changement de variables inversible à coefficients rationnelles qui réduit F à la forme normale de Weierstrass

$$Y^2Z - X^3 - aXZ^2 - bZ^3 \qquad (a, b \in \mathbb{Q}). \tag{14.2}$$

On peut aussi supposer que la solution rationnelle de depart devient la solution évidente $(0 : 1 : 0)$ de l'équation ainsi obtenue (14.2). La condition de non-singularité de (14.2) est équivalente à la non-annulation du discriminant $4a^3 + 27b^2$. Une courbe cubique plane non-singulière est dite *elliptique*, s'elle possède un point rationnel. En utilisant les coordonnées affines $x = X/Z, y = Y/Z$ on réduit $F = 0$ à la forme suivante :

$$y^2 = x^3 + ax + b, \tag{14.3}$$

où le polynôme cubique dans la partie droite n'a pas de racines multiples. Sous cette forme affine, la solution rationnelle ci-dessus devient le point à l'infinie O. Il existe une jolie description gométrique de la loi de composition sur l'ensemble des points rationnels de $\mathcal{C}$ qui devient un groupe abélien avec le point à l'infinie O comme l'élément neutre. Cette loi est donnée par la "méthode de sécantes et tangentes" de Poincaré. Notamment, pour une pair de points $P, Q \in \mathcal{C}(\mathbb{Q})$, on construit d'abord une droite passant par P, Q. Une telle droite intersecte aussi $\mathcal{C}$ en un troisième point bien définie P'. Ensuite, on construit de nouveau une droite passant par P' et O. Enfin, son troisème point d' intersection avec $\mathcal{C}$ est dit la somme $P + Q$. Si $P = Q$, la première droite à construire doit bien-sûr etre tangente à $\mathcal{C}$ en P.



Un calcul simple en coordonnées affines $P = (x_1, y_1),\ Q = (x_2, y_2)$ montre que $P + Q = (x_3, y_3)$ où

$$x_3 = -x_1 - x_2 + \left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2,$$
$$y_3 = \frac{y_1 - y_2}{x_1 - x_2}(x_1 - x_3) - y_1. \tag{14.4}$$

Dans le cas limite $P = Q$ on remarque que $2y'_x y = 3x^2 + a$, et on obtient

$$x_3 = -2x_1 + \left(\frac{3x_1^2 + a}{2y_1}\right)^2,\ y_3 = \frac{3x_1^2 + a}{2y_1}(x_1 - x_3) - y_1. \tag{14.5}$$

Si $x_1 = x_2$ et $y_1 = -y_2$ alors $P + Q = O$, est le point à l'infinie, qui est l'élément neutre pour la loi de groupe.

Cette méthode nous permet de construir de nouveaux points rationnels à partir des points connues. Tels points forment un sous-groupe engendré par des points de départ, par exemple, $mP,\ m \in \mathbb{Z}$, à partir juste un seul point P.

Pour les courbes cubiques singulières cette construction ne marche pas. Par exemple, on considère la courbe

$$\mathcal{C} :\ y^2 = x^2 + x^3, \tag{14.6}$$

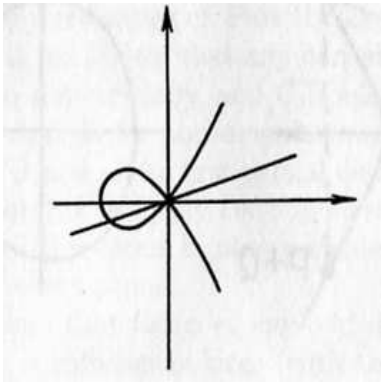


figure 8.

qui est représentée par Fig. 8. Toute droite passant par $(0, 0)$ n'a qu'un seul autre point d'intersection avec $\mathcal{C}$: sur $y = tx$ il est donné par l'équation $x^2(t^2 - x - 1) = 0$. A part de la solution triviale $x = 0$, on obtient $x = t^2 - 1$ et $y = t(t^2 - 1)$ donc nous avons trouvé tous les points sur $\mathcal{C}$ à l'aide d'une parametrisation rationnelle. Dans le cas non-singulier il n'existe pas de telle parametrisation.

Une courbe admettant une parametrisation rationnelle est dite une courbe rationnelle. Rapellons qu'un autre exemple d'une courbe rationnelle est donné par une conique plane et sa projection stéréographique.

La structure de groupe des points rationnels sur une cubique plane

Une propriété très remarquable de la "méthode de sécantes et tangentes" de Poincaré est que cette méthode nous permet de construir tous les points rationnels à partir d'un nombre fini des points rationnels. De point de vue de la théorie des groupes, cela signifie, que le résultat suivant a lieu :

Théorème 14.4.1 (Mordell, 1922) *Le groupe abélien $\mathcal{C}(\mathbb{Q})$ est de génération finie.*

On obtient alors du théorème de structure des groupes abéliens que

$$\mathcal{C}(\mathbb{Q}) \cong \Delta \times \mathbb{Z}^r$$

où Δ est le sous-groupe fini formé par les points de torsion, et $\mathbb{Z}^r$ est le produit de r copies du groupe cyclique infini. Le nombre r est dit le rang de $\mathcal{C}$ sur $\mathbb{Q}$. Il est connu que le groupe de torsion Δ peut être déterminée explicitement. Par exemple, Nagell et Lutz (Lutz E. (1937)) ont démontré que les points de torsion d'une courbe $y^2 = x^3 + ax + b$ avec a et b des nombres entiers, ont les coordonnées entiers x, y. De plus, l'ordonnée y d'un point de torsion soit nulle soit divise le nombre entier $D = -4a^3 - 27b^2$.

B.Mazur a démontré en 1976 que le sous-groupe de torsion Δ sur $\mathbb{Q}$ est isomorphe a l'un des quinze groupes suivants :

$$\mathbb{Z}/m\mathbb{Z}\ (m \leq 10, m = 12),\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}\ (n \leq 4), \tag{14.7}$$

et toutes ces possibilitées se réalisent.

Une question ouverte importante est si r peut être infiniement grand. En 1982 J.-L. Mestre a construit des exemples de courbes de rang au moins 14. Il a donné aussi un exemple relativement simple d'une courbe de rang ≥ 9 : $y^2 + 9767y = x^3 + 3576x^2 + 425x - 2412$.

En 2000 Martin – Mcmillen ont trouvé une courbe elliptique de rang ≥ 24 :

$$\begin{aligned} y^2 \quad & +xy + y = x^3 - 120039822036992245303534619191166796374x \\ & +504224992484910670010801799168082726759443756222911415116 \end{aligned}$$

(voir `http ://www.math.hr/ duje/tors/rankhist.html` pour d'autres exemples).

Exemples.

1. Soit $\mathcal{C}$ donnée par l'équation
$$y^2 + y = x^3 - x.$$
dont les solutions en nombre entiers donnent la liste des cas où le produit de deux entiers consecutifs est égale au produit de trois entiers consecutifs. Alors le groupe Δ est trivial et $\mathcal{C}(\mathbb{Q})$ est cyclique de générateur $P = (0, 0)$.

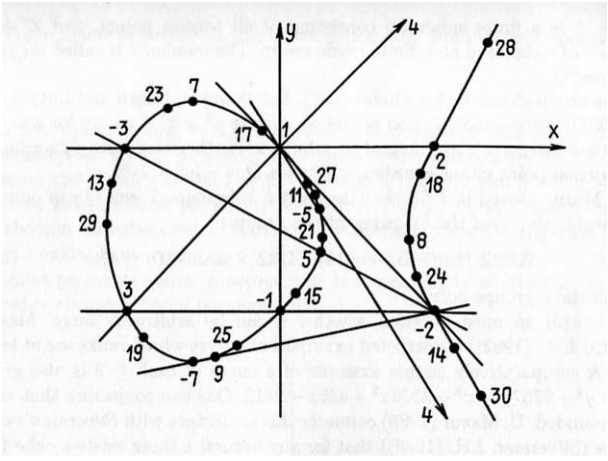


figure 9.

2. Les points mP (numérotés par m) sont montrés dans le Figure 9.
3. Soit $\mathcal{C}$ donnée par l'équation
$$y^2 + y = x^3 - 7x + 6.$$
Alors $\mathcal{C}(\mathbb{Q}) \cong \mathbb{Z}^3$, et les points (1,0), (6,0), (0,2) forment une base de ce groupe.

4. Considérons la courbe $y^2 = x^3 + px,\ p = 877$. Un générateur modulo torsion du groupe des points rationnels de cette courbe a l'abscisse x

$$x = \frac{375494528127162193105504069942092792346201}{6215987776871505425463220780697238044100}.$$

Cet exemple montre que les méthodes naives de recherche des ponts rationnels deviennent rapidement inefficace.

Congruences cubiques modulo un nombre premier p

Soit p un nombre premier et soit $F(X_0, X_1, X_2)$ une forme cubique à coefficients entiers. La réduction de F modulo p, donne une forme cubique sur le corps fini $\mathbb{F}_p$. Cette reduction est dit non-singulère s'elle n'a pas de zéros communs avec ces dérivées partielles dans toute extension de $\mathbb{F}_p$. On peut montrer que la plupart des résultats de la géométrie algébrique complexe restent valable sur les corps de caractéristique positive. Cependant, les formes normales d'une courbe elliptique sont légérement plus compliquées. En utilisant un changement de variables inversible des coordonneés projectives, on peut toujours réduire l'équation $F = 0$ en coordonnées affines à l'un des types suivantes(Koblitz N. (1987)) :

1. Pour $p \neq 2, 3$:

$$y^2 = x^3 + ax + b\ (4a^3 + 27b^2 \neq 0),\ a, b \in \mathbb{F}_p. \tag{14.8}$$

(on interdit le cas des racines multiples).

2. Pour $p = 2$:

$$y^2 + y = x^3 + ax + b,\ a, b \in \mathbb{F}_2 \tag{14.9}$$

(on n'a plus besoin d'exclure ici le cas des racines multiples).

3. Pour $p = 3$:

$$y^2 = x^3 + ax^2 + bx + c,\ a, b, c \in \mathbb{F}_3 \tag{14.10}$$

(on reinterdit le cas des racines multiples).

La courbe projective ainsi défini possède toujours le point $O = (0 : 1 : 0)$, rationnel sur $\mathbb{F}_p$ (rappelons que l'ensemble $\mathcal{C}(\mathbb{F}_p)$ des points rationnels sur $\mathbb{F}_p$ d'une courbe projective $\mathcal{C}\ : F(X, Y, Z) = 0$ est le sous-ensemble de $\mathbb{P}^2_{\mathbb{F}_p}$ des points

$$\Big\{(X : Y : Z) \in \mathbb{P}^2_{\mathbb{F}_p} \mid F(X, Y, Z) = 0\Big\}$$

Combien de points sur $\mathbb{F}_p$, c'est à dire, combien de solutions projectives de la congruence $F \equiv 0 \bmod\ p$, peut-on avoir ? Bien evidemment, le nombre total est au plus $2p + 1$ (on compt O), puisque sous la forme affine tout point fini x donne au plus deux valeurs de y. D'un autre coté, seulement une moitié des classes résiduelles sont les carrés (pour p impaire). Donc on peut espérer que $x^3 + ax + b$ est un carré pour environ une moitié des x'.

Plus précisemment, soit $\chi(x) = \left(\frac{x}{p}\right)$ le symbole de Legendre (8.1). Alors on a par la définition, que le nombre de solutions de $y^2 = u$ dans $\mathbb{F}_p$ est $1 + \chi(u)$. Ceci implique,

$$\begin{aligned}\text{Card}\ \mathcal{C}(\mathbb{F}_p) &= 1 + \sum_{x \in \mathbb{F}_p} (1 + \chi(x^3 + ax + b)) \\ &= p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax + b}{p}\right).\end{aligned}$$

N. Koblitz (1987) compare la dernière somme avec un résultat sur les marches aléatoires sur une droite. Après p marches on peut espérer d'être à distance environ $\sqrt{p}$ de zéro. En fait, on peut démontrer le théorème suivant remarquable :

THÉORÈME 14.4.2 (H.HASSE (1937)) *Soit* $N_p = \text{Card } \mathcal{C}(\mathbb{F}_p)$. *Alors*

$$|N_p - (p+1)| \leq 2\sqrt{p}.$$

Un preuve élémentaire a été donné par Yu.I.Manin (1956).

REMARQUE. Les courbes elliptiques sur les corps finis trouvent beaucoup d'applications. En particulier, les cas où un tel groupe est cyclique de grand taille amènent au cryptosystèmes ECDLP ("Elliptic curve discrete logarithm problem"), voir [Kob87].

EXERCICES

14.1 On considère la courbe affine sur $\mathbb{Q}$ donnée par l'équation

$$\mathcal{C} : 2x^2 + 3y^2 = 5.$$

(a) Montrer qu'il existe un point rationnel $(x_0, y_0) \in \mathcal{C}(\mathbb{Q})$.
(b) Soit $t \in \mathbb{Q}$. Trouver tous les points d'intersection de la droite

$$y - y_0 = t(x - x_0)$$

avec la courbe $\mathcal{C}(\mathbb{Q})$.
(c) En déduire une parametrisation rationnelle de la courbe $\mathcal{C}$.
(d) Trouver tous les points rationnels de la courbe projective, donnée par l'équation homogène $2X^2+3Y^2-5Z^2 = 0$.

14.2 On considère la courbe affine sur $\mathbb{F}_{49}$, donnée par l'équation

$$\mathcal{C} : 2x^2 + 3y^2 = 5.$$

(a) Montrer qu'il existe un point rationnel $(x_0, y_0) \in \mathcal{C}(\mathbb{F}_{49})$.
(b) Soit $t \in \mathbb{F}_{49}$. Trouver tous les points d'intersection de la droite

$$y - y_0 = t(x - x_0)$$

avec la courbe $\mathcal{C}(\mathbb{F}_{49})$.
(c) En déduire une parametrisation rationnelle sur $\mathbb{F}_{49}$ de la courbe $\mathcal{C}$.
(d) Trouver tous les points rationnels sur $\mathbb{F}_{49}$ de la courbe projective donnée par l'équation homogène $2X^2 + 3Y^2 - 5Z^2 = 0$.

14.3 On considère la courbe cubique plane $\mathcal{E} \subset \mathbb{P}^2$ sur $\mathbb{Q}$, donnée sous la forme affine suivante $y^2 = x(x+9)(x-16)$.
(a) Trouver l'equation de $\mathcal{E}$ en coordonnées projectives.
(b) Montrer que la courbe $\mathcal{E}$ est lisse.
(c) Montrer que l'ensemble

$$G = \{(\infty, \infty), (0,0), (0,-9), (0,16), (-4,20), (-4,-20), (36,180), (36,-180)\} \subset \mathbb{P}^2$$

est un sous-groupe de $\mathcal{E}(\mathbb{Q})$.
(d) Le groupe G est-il cyclique ?

14.4 On considère une courbe cubique plane $\mathcal{F} \subset \mathbb{P}^2$ sur $\mathbb{F}_4$, donnée sous la forme affine suivante $y^2+y = x^3+x+1$.
(a) Montrer que la courbe $\mathcal{F}$ est lisse.
(b) Trouver l'ordre du groupe $H = \mathcal{F}(\mathbb{F}_4)$.
(c) Le groupe H est-il cyclique ?

14.5 Points des courbes algébriques sur les corps finis (exemples)

COURBE de FERMAT sur GF(4)

$$x^3 + y^3 + z^3 = 0$$

```
> restart ;
> with(linalg) :
```

```
Warning, the protected names norm and trace have been redefined and
unprotected
```

```
> g:=x^2+x+1 mod 2;
```

$$g := x^2 + x + 1$$

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

$$\alpha$$

```
> f:=(x,y,z)->x^3+y^3+z^3;
```

$$f := (x,\, y,\, z) \to x^3 + y^3 + z^3$$

```
> h:=(i,j)->x[i-1,j-1]: X:=Matrix(3,2,h);
```

$$X := \begin{bmatrix} x_{0,0} & x_{0,1} \\ x_{1,0} & x_{1,1} \\ x_{2,0} & x_{2,1} \end{bmatrix}$$

```
> u:=(i,j)-> alpha^(i-1):U:=Matrix(2,1,u);
```

$$U := \begin{bmatrix} 1 \\ \alpha \end{bmatrix}$$

```
> with(LinearAlgebra):
> Y:= Multiply(X, U);
```

$$Y := \begin{bmatrix} x_{0,0} + x_{0,1}\,\alpha \\ x_{1,0} + x_{1,1}\,\alpha \\ x_{2,0} + x_{2,1}\,\alpha \end{bmatrix}$$

```
> v[1]:=f(0, 1, x[2]);
```

$$v_1 := 1 + {x_2}^3$$

```
> v[2]:=f(1, x[1], x[2]);
```

$$v_2 := 1 + {x_1}^3 + {x_2}^3$$

```
> vv[1]:=subs(x[0]=Y[1,1],x[1]=Y[2,1], x[2]=Y[3,1],v[1]) ;
```

$$vv_1 := 1 + (x_{2,0} + x_{2,1}\,\alpha)^3$$

```
> vv[2]:= subs(x[0]=Y[1,1],x[1]=Y[2,1], x[2]=Y[3,1],v[2]) ;
```

$$vv_2 := 1 + (x_{1,0} + x_{1,1}\,\alpha)^3 + (x_{2,0} + x_{2,1}\,\alpha)^3$$

```
> c:=0;
> if f(0,0,1) mod 2 =0 then c:=c+1;
> print (c, [0, 0, 1]) fi;
> for i from 0 to 1 do
> for j from 0 to 1 do
> if Eval(vv[1],{x[2,0]=i,x[2,1]=j}) mod 2 =0 then c:=c+1;
> print (c,[0, 1, i+j*alpha]) fi ;od ;od;
> for i2 from 0 to 1 do
> for j2 from 0 to 1 do
> for i1 from 0 to 1 do
> for j1 from 0 to 1 do
> if Eval(vv[2],{x[2,0]=i2,x[2,1]=j2, x[1,0]=i1,x[1,1]=j1}) mod 2
> =0 then c:=c+1;
> print (c,[1, (i1+j1*alpha)mod 2,
> (i2+j2*alpha)mod 2]) fi od; od ;od ;od;
```

$$c := 0$$

$$1,\ [0,\ 1,\ \alpha]$$

$$2,\ [0,\ 1,\ 1]$$

$$3,\ [0,\ 1,\ 1+\alpha]$$

$$4,\ [1,\ \alpha,\ 0]$$

$$5,\ [1,\ 1,\ 0]$$

$$6,\ [1,\ 1+\alpha,\ 0]$$

$$7,\ [1,\ 0,\ \alpha]$$

$$8,\ [1,\ 0,\ 1]$$

$$9,\ [1,\ 0,\ 1+\alpha]$$

COURBE de FERMAT sur GF(16)

$$x^3 + y^3 + z^3 = 0$$

```
> restart ;
> with(linalg) :

Warning, the protected names norm and trace have been redefined and
unprotected

> g:=x^4+x+1 mod 2;
```

$$g := x^4 + x + 1$$

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

$$\alpha$$

```
> f:=(x,y,z)->x^3+y^3+z^3;
```

$$f := (x,\ y,\ z) \to x^3 + y^3 + z^3$$

```
> h:=(i,j)->x[i-1,j-1]: X:=Matrix(3,4,h);
```

$$X := \begin{bmatrix} x_{0,0} & x_{0,1} & x_{0,2} & x_{0,3} \\ x_{1,0} & x_{1,1} & x_{1,2} & x_{1,3} \\ x_{2,0} & x_{2,1} & x_{2,2} & x_{2,3} \end{bmatrix}$$

```
> u:=(i,j)-> alpha^(i-1):U:=Matrix(4,1,u);
```

$$U := \begin{bmatrix} 1 \\ \alpha \\ \alpha^2 \\ \alpha^3 \end{bmatrix}$$

```
> with(LinearAlgebra):
> Y:= Multiply(X, U);
```

```
Warning, the assigned name GramSchmidt now has a global binding
```

$$Y := \begin{bmatrix} x_{0,0} + x_{0,1}\,\alpha + x_{0,2}\,\alpha^2 + x_{0,3}\,\alpha^3 \\ x_{1,0} + x_{1,1}\,\alpha + x_{1,2}\,\alpha^2 + x_{1,3}\,\alpha^3 \\ x_{2,0} + x_{2,1}\,\alpha + x_{2,2}\,\alpha^2 + x_{2,3}\,\alpha^3 \end{bmatrix}$$

```
> v[1]:=f(0, 1, x[2]);
```

$$v_1 := 1 + {x_2}^3$$

```
> v[2]:=f(1, x[1], x[2]);
```

$$v_2 := 1 + {x_1}^3 + {x_2}^3$$

```
> vv[1]:=subs(x[0]=Y[1,1],x[1]=Y[2,1], x[2]=Y[3,1],v[1]) ;
```

$$vv_1 := 1 + (x_{2,0} + x_{2,1}\,\alpha + x_{2,2}\,\alpha^2 + x_{2,3}\,\alpha^3)^3$$

```
> vv[2]:= subs(x[0]=Y[1,1],x[1]=Y[2,1], x[2]=Y[3,1],v[2]) ;
```

$$vv_2 := 1 + (x_{1,0} + x_{1,1}\,\alpha + x_{1,2}\,\alpha^2 + x_{1,3}\,\alpha^3)^3 + (x_{2,0} + x_{2,1}\,\alpha + x_{2,2}\,\alpha^2 + x_{2,3}\,\alpha^3)^3$$

```
> c:=0;
> if f(0,0,1) mod 2 =0 then c:=c+1;
> print (c, [0, 0, 1]) fi;
> for i from 0 to 1 do
> for j from 0 to 1 do
> for k from 0 to 1 do
> for l from 0 to 1 do
> if Eval(vv[1],{x[2,0]=i,x[2,1]=j,x[2,2]=k,x[2,3]=l}) mod 2 =0
> then c:=c+1;
> print (c,[0, 1,
> i+j*alpha+k*alpha^2+l*alpha^3]) fi; od; od ;od ;od;
> for i2 from 0 to 1 do
> for j2 from 0 to 1 do
> for k2 from 0 to 1 do
> for l2 from 0 to 1 do
> for i1 from 0 to 1 do
> for j1 from 0 to 1 do
> for k1 from 0 to 1 do
> for l1 from 0 to 1 do
> if Eval(vv[2],{x[2,0]=i2,x[2,1]=j2,x[2,2]=k2,x[2,3]=l2,
> x[1,0]=i1,x[1,1]=j1,x[1,2]=k1,x[1,3]=l1}) mod 2 =0 then c:=c+1;
> print (c,[1,
> i1+j1*alpha+k1*alpha^2+l1*alpha^3, i2+j2*alpha+k2*alpha^2+l2*alpha^3])
> fi; od; od ;od ;od;od;od;od; od;
```

$$c := 0$$

$$1,\ [0,\ 1,\ \alpha + \alpha^2]$$

$$2,\ [0,\ 1,\ 1]$$

$$3,\ [0,\ 1,\ 1 + \alpha + \alpha^2]$$

$$4,\ [1,\ \alpha + \alpha^2,\ 0]$$

$$5,\ [1,\ 1,\ 0]$$
$$6,\ [1,\ \alpha+\alpha^2+1,\ 0]$$
$$7,\ [1,\ 0,\ \alpha^2+\alpha]$$
$$8,\ [1,\ 0,\ 1]$$
$$9,\ [1,\ 0,\ \alpha+1+\alpha^2]$$

COURBE de KLEIN sur GF(16)

$$x^3y+y^3z+z^3x=0$$

```
> fk:=(x,y,z)->x^3*y+y^3*z+z^3*x;
```

$$fk := (x,\ y,\ z) \to x^3\,y+y^3\,z+z^3\,x$$

```
> vk[1]:=fk(0, 1, x[2]);
```

$$vk_1 := x_2$$

```
> vk[2]:=fk(1, x[1], x[2]);
```

$$vk_2 := x_1+{x_1}^3\,x_2+{x_2}^3$$

```
> vvk[1]:=subs(x[0]=Y[1,1],x[1]=Y[2,1], x[2]=Y[3,1],vk[1]) ;
```

$$vvk_1 := x_{2,\,0}+x_{2,\,1}\,\alpha+x_{2,\,2}\,\alpha^2+x_{2,\,3}\,\alpha^3$$

```
> vvk[2]:= subs(x[0]=Y[1,1],x[1]=Y[2,1], x[2]=Y[3,1],vk[2]) ;
```

$$\begin{aligned} vvk_2 := {} & x_{1,\,0}+x_{1,\,1}\,\alpha+x_{1,\,2}\,\alpha^2+x_{1,\,3}\,\alpha^3 \\ & +(x_{1,\,0}+x_{1,\,1}\,\alpha+x_{1,\,2}\,\alpha^2+x_{1,\,3}\,\alpha^3)^3\,(x_{2,\,0}+x_{2,\,1}\,\alpha+x_{2,\,2}\,\alpha^2+x_{2,\,3}\,\alpha^3) \\ & +(x_{2,\,0}+x_{2,\,1}\,\alpha+x_{2,\,2}\,\alpha^2+x_{2,\,3}\,\alpha^3)^3 \end{aligned}$$

```
> c:=0;
> if fk(0,0,1) mod 2 =0 then c:=c+1;
> print (c, [0, 0, 1]) fi;
> for i from 0 to 1 do
> for j from 0 to 1 do
> for k from 0 to 1 do
> for l from 0 to 1 do
> if Eval(vvk[1],{x[2,0]=i,x[2,1]=j,x[2,2]=k,x[2,3]=l}) mod 2 =0
> then c:=c+1;
> print (c,[0, 1,
> i+j*alpha+k*alpha^2+l*alpha^3]) fi; od; od ;od ;od;
> for i2 from 0 to 1 do
> for j2 from 0 to 1 do
> for k2 from 0 to 1 do
> for l2 from 0 to 1 do
> for i1 from 0 to 1 do
> for j1 from 0 to 1 do
> for k1 from 0 to 1 do
> for l1 from 0 to 1 do
> if Eval(vvk[2],{x[2,0]=i2,x[2,1]=j2,x[2,2]=k2,x[2,3]=l2,
> x[1,0]=i1,x[1,1]=j1,x[1,2]=k1,x[1,3]=l1}) mod 2 =0 then c:=c+1;
> print (c,[1,
> i1+j1*alpha+k1*alpha^2+l1*alpha^3, i2+j2*alpha+k2*alpha^2+l2*alpha^3])
> fi; od; od ;od ;od;od;od;od; od;
```

$$c := 0$$

$$c := 1$$

$$1,\ [0,\ 0,\ 1]$$

$$2,\ [0,\ 1,\ 0]$$

$$3,\ [1,\ 0,\ 0]$$

$$4,\ [1,\ 1+\alpha^2,\ \alpha^3]$$

$$5,\ [1,\ \alpha,\ \alpha^3+\alpha^2]$$

$$6,\ [1,\ \alpha+1,\ \alpha+\alpha^3]$$

$$7,\ [1,\ \alpha^3,\ \alpha+\alpha^2]$$

$$8,\ [1,\ 1+\alpha^2+\alpha,\ \alpha+\alpha^2]$$

$$9,\ [1,\ 1+\alpha+\alpha^2+\alpha^3,\ \alpha+\alpha^2]$$

$$10,\ [1,\ \alpha+\alpha^2,\ \alpha^3+\alpha+\alpha^2]$$

$$11,\ [1,\ \alpha^2+\alpha,\ \alpha^3+1]$$

$$12,\ [1,\ 1+\alpha+\alpha^2,\ \alpha^3+1+\alpha^2]$$

$$13,\ [1,\ \alpha+\alpha^2+1,\ 1+\alpha^3+\alpha]$$

$$14,\ [1,\ \alpha^3+\alpha^2,\ \alpha+\alpha^2+1]$$

$$15,\ [1,\ \alpha+\alpha^3,\ \alpha+\alpha^2+1]$$

$$16,\ [1,\ \alpha+\alpha^2,\ \alpha+\alpha^2+1]$$

$$17,\ [1,\ \alpha^2,\ 1+\alpha+\alpha^2+\alpha^3]$$

COURBE de KLEIN sur GF(8)

$$x^3y + y^3z + z^3x = 0$$

```
> restart ;
> with(linalg) :
```

```
Warning, the protected names norm and trace have been redefined and
unprotected
```

```
> g:=x^3+x+1 mod 2;
```

$$g := x^3 + x + 1$$

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

$$\alpha$$

```
> fk:=(x,y,z)->x^3*y+y^3*z+z^3*x;
```

$$fk := (x,\ y,\ z) \rightarrow x^3\,y + y^3\,z + z^3\,x$$

```
> h:=(i,j)->x[i-1,j-1]: X:=Matrix(3,3,h);
```

$$X := \begin{bmatrix} x_{0,0} & x_{0,1} & x_{0,2} \\ x_{1,0} & x_{1,1} & x_{1,2} \\ x_{2,0} & x_{2,1} & x_{2,2} \end{bmatrix}$$

```
> u:=(i,j)-> alpha^(i-1):U:=Matrix(3,1,u);
```

$$U := \begin{bmatrix} 1 \\ \alpha \\ \alpha^2 \end{bmatrix}$$

```
> with(LinearAlgebra):
> Y:= Multiply(X, U);
```

```
Warning, the assigned name GramSchmidt now has a global binding
```

$$Y := \begin{bmatrix} x_{0,0} + x_{0,1}\,\alpha + x_{0,2}\,\alpha^2 \\ x_{1,0} + x_{1,1}\,\alpha + x_{1,2}\,\alpha^2 \\ x_{2,0} + x_{2,1}\,\alpha + x_{2,2}\,\alpha^2 \end{bmatrix}$$

```
> vk[1]:=fk(0, 1, x[2]);
```

$$vk_1 := x_2$$

```
> vk[2]:=fk(1, x[1], x[2]);
```

$$vk_2 := x_1 + {x_1}^3\,x_2 + {x_2}^3$$

```
> vvk[1]:=subs(x[0]=Y[1,1],x[1]=Y[2,1], x[2]=Y[3,1],vk[1]) ;
```

$$vvk_1 := x_{2,0} + x_{2,1}\,\alpha + x_{2,2}\,\alpha^2$$

```
> vvk[2]:= subs(x[0]=Y[1,1],x[1]=Y[2,1], x[2]=Y[3,1],vk[2]) ;
```

$$vvk_2 := x_{1,0} + x_{1,1}\,\alpha + x_{1,2}\,\alpha^2 + (x_{1,0} + x_{1,1}\,\alpha + x_{1,2}\,\alpha^2)^3\,(x_{2,0} + x_{2,1}\,\alpha + x_{2,2}\,\alpha^2) + (x_{2,0} + x_{2,1}\,\alpha + x_{2,2}\,\alpha^2)^3$$

```
> c:=0;
> if fk(0,0,1) mod 2 = 0 then c:=c+1;
> print (c,  [0, 0, 1]) fi;
> for i from 0 to 1 do
> for j from 0 to 1 do
> for k from 0 to 1 do
> if Eval(vvk[1],{x[2,0]=i,x[2,1]=j,x[2,2]=k}) mod 2 =0 then
> c:=c+1;
> print (c,  [0, 1, i+j*alpha+k*alpha^2])
> fi; od; od ;od ;
> for i2 from 0 to 1 do
> for j2 from 0 to 1 do
> for k2 from 0 to 1 do
> for i1 from 0 to 1 do
> for j1 from 0 to 1 do
> for k1 from 0 to 1 do
> if Eval(vvk[2],{x[2,0]=i2,x[2,1]=j2,x[2,2]=k2,
> x[1,0]=i1,x[1,1]=j1,x[1,2]=k1}) mod 2 =0 then c:=c+1;
> print (c, [1, i1+j1*alpha+k1*alpha^2,
> i2+j2*alpha+k2*alpha^2]) fi; od; od ;od ;od;od;od;
```

$$c := 0$$

$$c := 1$$

$$1,\ [0,\ 0,\ 1]$$

$$2,\ [0,\ 1,\ 0]$$

$$3,\ [1,\ 0,\ 0]$$

$$4,\ [1,\ \alpha,\ \alpha^2]$$

$$5,\ [1,\ 1,\ \alpha^2]$$

$$6,\ [1,\ 1+\alpha,\ \alpha^2]$$

$$7,\ [1,\ \alpha^2+\alpha,\ \alpha]$$
$$8,\ [1,\ 1,\ \alpha]$$
$$9,\ [1,\ 1+\alpha+\alpha^2,\ \alpha]$$
$$10,\ [1,\ \alpha^2,\ \alpha^2+\alpha]$$
$$11,\ [1,\ 1,\ \alpha^2+\alpha]$$
$$12,\ [1,\ 1+\alpha^2,\ \alpha^2+\alpha]$$
$$13,\ [1,\ \alpha^2,\ 1]$$
$$14,\ [1,\ \alpha,\ 1]$$
$$15,\ [1,\ \alpha^2+\alpha,\ 1]$$
$$16,\ [1,\ \alpha,\ 1+\alpha^2]$$
$$17,\ [1,\ 1+\alpha^2,\ 1+\alpha^2]$$
$$18,\ [1,\ 1+\alpha+\alpha^2,\ 1+\alpha^2]$$
$$19,\ [1,\ \alpha^2+\alpha,\ 1+\alpha]$$
$$20,\ [1,\ 1+\alpha^2,\ 1+\alpha]$$
$$21,\ [1,\ 1+\alpha,\ 1+\alpha]$$
$$22,\ [1,\ \alpha^2,\ 1+\alpha+\alpha^2]$$
$$23,\ [1,\ 1+\alpha,\ 1+\alpha+\alpha^2]$$
$$24,\ [1,\ 1+\alpha+\alpha^2,\ 1+\alpha+\alpha^2]$$

COURBE de FERMAT sur GF(8)

```
> restart ;
> with(linalg) :
```

```
Warning, the protected names norm and trace have been redefined and
unprotected
```

```
> g:=x^3+x+1 mod 2;
```

$$g := x^3 + x + 1$$

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

$$\alpha$$

```
> f:=(x,y,z)->x^3+y^3+z^3;
```

$$f := (x,\ y,\ z) \to x^3 + y^3 + z^3$$

```
> h:=(i,j)->x[i-1,j-1]: X:=Matrix(3,3,h);
```

$$X := \begin{bmatrix} x_{0,0} & x_{0,1} & x_{0,2} \\ x_{1,0} & x_{1,1} & x_{1,2} \\ x_{2,0} & x_{2,1} & x_{2,2} \end{bmatrix}$$

```
> u:=(i,j)-> alpha^(i-1):U:=Matrix(3,1,u);
```

$$U := \begin{bmatrix} 1 \\ \alpha \\ \alpha^2 \end{bmatrix}$$

```
> with(LinearAlgebra):
> Y:= Multiply(X, U);
```

```
Warning, the assigned name GramSchmidt now has a global binding
```

$$Y := \begin{bmatrix} x_{0,0} + x_{0,1}\,\alpha + x_{0,2}\,\alpha^2 \\ x_{1,0} + x_{1,1}\,\alpha + x_{1,2}\,\alpha^2 \\ x_{2,0} + x_{2,1}\,\alpha + x_{2,2}\,\alpha^2 \end{bmatrix}$$

```
> v[1]:=f(0, 1, x[2]);
```

$$v_1 := 1 + {x_2}^3$$

```
> v[2]:=f(1, x[1], x[2]);
```

$$v_2 := 1 + {x_1}^3 + {x_2}^3$$

```
> vv[1]:=subs(x[0]=Y[1,1],x[1]=Y[2,1], x[2]=Y[3,1],v[1]) ;
```

$$vv_1 := 1 + (x_{2,0} + x_{2,1}\,\alpha + x_{2,2}\,\alpha^2)^3$$

```
> vv[2]:= subs(x[0]=Y[1,1],x[1]=Y[2,1], x[2]=Y[3,1],v[2]) ;
```

$$vv_2 := 1 + (x_{1,0} + x_{1,1}\,\alpha + x_{1,2}\,\alpha^2)^3 + (x_{2,0} + x_{2,1}\,\alpha + x_{2,2}\,\alpha^2)^3$$

```
> c:=0;
> for i from 0 to 1 do
> for j from 0 to 1 do
> for k from 0 to 1 do
> if Eval(vv[1],{x[2,0]=i,x[2,1]=j,x[2,2]=k}) mod 2 =0 then
> c:=c+1;
> print (c,[0, 1, i+j*alpha+k*alpha^2])
> fi; od; od ;od ;
> for i from 0 to 1 do
> for j from 0 to 1 do
> for k from 0 to 1 do
> for i1 from 0 to 1 do
> for j1 from 0 to 1 do
> for k1 from 0 to 1 do
> if Eval(vv[2],{x[2,0]=i,x[2,1]=j,x[2,2]=k,
> x[1,0]=i1,x[1,1]=j1,x[1,2]=k1}) mod 2 =0 then c:=c+1;
> print (c,[1, (i1+j1*alpha+k1*alpha^2)
> mod 2 ,(i+j*alpha+k*alpha^2) mod 2]) fi; od; od ;od ;od;od;od;
```

$$c := 0$$

$$1,\ [0,\ 1,\ 1]$$

$$2,\ [1,\ 1,\ 0]$$

$$3,\ [1,\ 1+\alpha,\ \alpha^2]$$

$$4,\ [1,\ \alpha^2+\alpha+1,\ \alpha]$$

$$5,\ [1,\ \alpha^2+1,\ \alpha+\alpha^2]$$

$$6,\ [1,\ 0,\ 1]$$

$$7,\ [1,\ \alpha+\alpha^2,\ 1+\alpha^2]$$

$$8,\ [1,\ \alpha^2,\ \alpha+1]$$

$$9,\ [1,\ \alpha,\ 1+\alpha+\alpha^2]$$

COURBE de FERMAT sur GF(9)

$$x^4 + y^4 + z^4 = 0$$

```
> restart ;
> with(linalg) :
> g:=x^2+1 mod 3;
```

```
Warning, the protected names norm and trace have been redefined and
unprotected
```

$$g := x^2 + 1$$

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

$$\alpha$$

```
> f:=(x,y,z)->x^4+y^4+z^4;
```

$$f := (x,\, y,\, z) \to x^4 + y^4 + z^4$$

```
> h:=(i,j)->x[i-1,j-1]: X:=Matrix(3,2,h);
```

$$X := \begin{bmatrix} x_{0,0} & x_{0,1} \\ x_{1,0} & x_{1,1} \\ x_{2,0} & x_{2,1} \end{bmatrix}$$

```
> u:=(i,j)-> alpha^(i-1):U:=Matrix(2,1,u);
```

$$U := \begin{bmatrix} 1 \\ \alpha \end{bmatrix}$$

```
> with(LinearAlgebra):
> Y:= Multiply(X, U);
```

```
Warning, the assigned name GramSchmidt now has a global binding
```

$$Y := \begin{bmatrix} x_{0,0} + x_{0,1}\,\alpha \\ x_{1,0} + x_{1,1}\,\alpha \\ x_{2,0} + x_{2,1}\,\alpha \end{bmatrix}$$

```
> v[1]:=f(0, 1, x[2]);
```

$$v_1 := 1 + {x_2}^4$$

```
> v[2]:=f(1, x[1], x[2]);
```

$$v_2 := 1 + {x_1}^4 + {x_2}^4$$

```
> vv[1]:=subs(x[0]=Y[1,1],x[1]=Y[2,1], x[2]=Y[3,1],v[1]) ;
```

$$vv_1 := 1 + (x_{2,0} + x_{2,1}\,\alpha)^4$$

```
> vv[2]:= subs(x[0]=Y[1,1],x[1]=Y[2,1], x[2]=Y[3,1],v[2]) ;
```

$$vv_2 := 1 + (x_{1,0} + x_{1,1}\,\alpha)^4 + (x_{2,0} + x_{2,1}\,\alpha)^4$$

```
> c:=0;
> for i from 0 to 2 do
> for j from 0 to 2 do
> if Eval(vv[1],{x[2,0]=i,x[2,1]=j}) mod 3 =0 then c:=c+1;
> print (c,[0, 1, i+j*alpha]) fi; od; od
> ;for i2 from 0 to 2 do
> for j2 from 0 to 2 do
> for i1 from 0 to 2 do
> for j1 from 0 to 2 do
> if Eval(vv[2],{x[2,0]=i2,x[2,1]=j2,x[1,0]=i1,x[1,1]=j1})
> mod 3 =0 then c:=c+1;
> print (c,[1, (i1+j1*alpha)mod 3
> ,(i2+j2*alpha) mod 3]) fi; od; od ;od ;od;
```

$$c := 0$$

$$1,\, [0,\, 1,\, 1 + \alpha]$$

2, $[0,\ 1,\ 1+2\,\alpha]$

3, $[0,\ 1,\ 2+\alpha]$

4, $[0,\ 1,\ 2+2\,\alpha]$

5, $[1,\ 1+\alpha,\ 0]$

6, $[1,\ 1+2\,\alpha,\ 0]$

7, $[1,\ 2+\alpha,\ 0]$

8, $[1,\ 2+2\,\alpha,\ 0]$

9, $[1,\ \alpha,\ \alpha]$

10, $[1,\ 2\,\alpha,\ \alpha]$

11, $[1,\ 1,\ \alpha]$

12, $[1,\ 2,\ \alpha]$

13, $[1,\ \alpha,\ 2\,\alpha]$

14, $[1,\ 2\,\alpha,\ 2\,\alpha]$

15, $[1,\ 1,\ 2\,\alpha]$

16, $[1,\ 2,\ 2\,\alpha]$

17, $[1,\ \alpha,\ 1]$

18, $[1,\ 2\,\alpha,\ 1]$

19, $[1,\ 1,\ 1]$

20, $[1,\ 2,\ 1]$

21, $[1,\ 0,\ 1+\alpha]$

22, $[1,\ 0,\ 1+2\,\alpha]$

23, $[1,\ \alpha,\ 2]$

24, $[1,\ 2\,\alpha,\ 2]$

25, $[1,\ 1,\ 2]$

26, $[1,\ 2,\ 2]$

27, $[1,\ 0,\ 2+\alpha]$

28, $[1,\ 0,\ 2+2\,\alpha]$

Références

[AGP94] Alford W.-R. Granville A. Pomerance C. There are infinitely many Carmichael numbers. Ann. Math. **139**, 703–722 (1994).

[AF] Jean-Marie Arnaudiès et Henri Fraysse *Algèbre*, Dunod, Paris, 1987. xi+691 pp.

[BS85] Borevich, Z.I., Shafarevich, I.R. Number Theory. (en russe). 3rd ed. Nauka, Moscow (1985). Traduction anglaise. : New York/London : Academic Press, 1966.

[Dem] Michel Demazure, *Cours d'algèbre. Primalité. Divisibilité. Codes.*, Nouvelle Bibliothèque Mathématique, 1. Cassini, Paris, 1997. xviii+302 pp.

[God] Roger Godement, *Cours d'algèbre.*, Hermann, Paris, 1969

[Kob87] Neal Koblitz, *A course of number theory and cryptography*, Graduate texts in mathematics 114, New York : Springer Verlag, 1987.

[Knu81] D.E. Knuth *The art of computer programming.* Vol **2**. Seminumerical algorithms. 2nd edition. Addison–Wesley, Reading (1981).

[La] Serge Lang , Algebra. Reading, Mass. : Addison–Wesley (1965).

[Li-Ni] Rudolf Lidl et Harald Niederreiter, *Introduction to finite fields and their applications.* Addison–Wesley : Reading, 1983

[Ma-Pa] Yu.I. Manin et A.A.Panchishkin, *Number Theory I : Introduction to Number Theory*, Encyclopaedia of Mathematical Sciences, vol. 49, Springer-Verlag, 1995, 303 p.

[Mon88] D. Monasse, *Mathématique et Informatique.* Classes préparatoires. Vuibert, 1988

[Pey] Emmanuel Peyre, *Corps finis et courbes elliptiques.* DESS Cryptologie, sécurité et codage d'information, Modules A1A et A1B, Grenoble, 2002, pp. 1-128

[RSA] R. L. Rivest, A. Shamir et L. M. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, CACM, 21,1978, 120–126

[Se70] J.– P. Serre, Cours d'arithmétique. Paris, Press Univ. France, 1970.

[Stein] William Stein, *An Explicit Approach to Number Theory* (à paraître, voir page internet : `http ://modular.fas.harvard.edu/edu/Fall2001/124/lectures`).

[Ste] S. A. Stepanov, *Codes on algebraic curves.* Kluwer Academic Publishers. vii, 350 p., 1999

[T-MF] Tenenbaum G., Mendes-France, *Les nombres premiers*, Collection Que Sais-Je, Paris, Press Univ. France, 1997

[VdW71] B.L. van der Waerden, *Algebra I,II*, New York : Springer Verlag, 1971, 1967.