LES CORPS FINIS

PHILIPPE LANGEVIN

Résumé.

1. Introduction

Le fameux théorème de Wedderburn affirme que pour les corps la finitude implique la commutativité. Un résultat plus facile à démontrer qu'à comprendre. De cette petite merveille mathématiques découle que l'univers des corps finis est relativement étroit du point de vue ensembliste. En effet, pour chaque puissance q d'un nombre premier p il existe une et une seule structure de corps fini : le corps de Galois à q éléments. À ce stade, les algébristes s'arrêttent et commence ce petit cours dont le seul but est de proposer l'essentiel des nombreuses propriétés cachées vérifiées par les corps finis ainsi que quelques applications en combinatoire algébrique. Un petit détour par les travaux des anciens : Fermat, Euler, Gauss etc... Une introduction à la méthode des sommes de caractères et des sommes de Gauss pour terminer avec trois résultats fondamentaux : le théorème d'Ax, la borne de Carlitz-Uchiyama et le théorème de Carlitz. Dans mon texte, je suppose le lecteur familier avec le langage de l'algèbre commutative. Il a déjà rencontré la notion de corps ! et plus généralement celles des anneaux de leurs idéaux, polynômes et autres quotients. Il ne maîtrise pas ces notions mais comprend la définition de Dicson :

2. Préliminaires

Comme d'habitude $\mathbf{Z}$ désigne l'ensemble des entiers relatifs qui, une fois muni des opérations d'addition et de multiplication, devient un annneau Euclidien. Etant donnés deux entiers relatifs a et b, b non nul, il existe un unique couple d'entiers naturels (q, r) vérifiant :

$$a = bq + r, \quad 0 \leq r < |b|. \tag{1}$$

L'entier q s'appelle le quotient de la division Euclidienne de a par b et r le reste.

Exercice 1. *soient a et b deux entiers. Montrer qu'il existe un et un sel couple d'entiers (q, r) satisfaisant les conditions :*

$$a = bq + r, \quad |r| \leq |\frac{b}{2}|. \tag{2}$$

Trouver (q, r) c'est effectuer la division à reste minimal de a par b.

Date: Septembre 1999.

Fixons m un entier positif. L'ensemble des restes possibles de la division Euclidienne par m est 0, 1, ..., $m-1$: c'est l'ensemble des résidus modulo m. À son tour, cet ensemble est muni de deux lois internes $\oplus$ et $\otimes$. Pout tout résidus r et s, la somme $r \oplus s$ est égal au reste de la division Euclidienne de $r+s$ par m, le produit $r \otimes s$ se définit de manière analogue. L'ensemble des résidus modulo m est un anneau fini commutatif noté $\mathbf{Z}/m\mathbf{Z}$, c'est le quotient de l'anneau $\mathbf{Z}$ par l'idéal $m\mathbf{Z}$.

Théorème 2.1. *Soit m un entier positif. L'anneau des résidus modulo m est un corps si et seulement si m est un nombre premier.*

Démonstration. La condition est nécessaire car un corps ne possède pas de diviseur de zéros. Réciproquement, étant donné un résidu non nul a modulo m, il s'agit de prouver l'existence d'un inverse et je propose au lecteur d'en faire trois différentes preuves.

(1) Considérer la multiplication par a.
(2) Examiner la suite des a^n.
(3) Utiliser l'identité de Bezout. □

Le troisième point est particulièrement interessant parce qu'il fournit un algorithme de calcul d'inverse modulo m.

À titre d'exercice, le lecteur prouvera le théorème de Wilson :

Proposition 1. *L'entier p est premier si et seulement si $(p-1)! \equiv -1 \mod m$.*

3. Le petit théorème de Fermat

Pour un nombre premier p, on préfère noter $\mathbf{F}_p$ le corps $\mathbf{Z}/(p)$. Le petit théorème de Fermat affirme que dans $\mathbf{F}_p$ on a l'identité :

$$\forall a \in \mathbf{F}_p, \quad a^p = a. \tag{3}$$

Il suffit de montrer que dans $\mathbf{F}_p$ l'élévation à la pouissance p vérifie $(a+b)^p = a^p + b^p$.

Soit m un entier. Est-il premier ? Du point de vue algorithmique, cette question est redoutable, le rôle d'un test de primalité est d'y répondre. On dit qu'un nombre m est pseudo-premier si $2^{m-1} \equiv 1 \mod m$. Du petit théorème de Fermat, on déduit qu'en particulier, tous les nombres premiers sont tous pseudo-premiers, la réciproque est fausse : trouvez un contre exemple ! Mais on démontre que la probabilité pour qu'un nombre pseudo premier soit non premier est trés faible.

4. Entiers de Gauss

Désignons par i une des deux racines carrées de -1 dans le corps des nombres complexes. L'ensemble $\{a+ib \mid a,b \in \mathbf{Z}\}$ muni des opérations usuelles est un sous-anneau du corps $\mathbf{C}$. C'est l'anneau des entiers de Gauss $\mathbf{Z}[i]$ dont le corps des fractions est $\{a+ib \mid a,b \in \mathbf{Q}\}$. Rappelons que le conjugué de $z = a+ib$ est $\bar{z} = a-ib$ et que la norme de z est $N(z) = z\bar{z} = a^2+b^2$. En partilier, la norme est une application multiplicative. En déduire,

Théorème 4.1. *L'anneau des entiers de Gauss est Euclidien. Etant donnés deux entiers de Gauss x et y, y non nul, il existe un couple (q, r) vérifiant*

$$x = qy + r, \quad 0 \leq r < N(y) \tag{4}$$

Démonstration. On écrit $x/y = a/n + ib/n$ où a, b sont deux entiers relatifs et n un entier positif. La division à reste minimal (2) permet d'érire

$$\begin{aligned} a &= qn + r, & |r| &\leq |\frac{n}{2}|; \\ b &= q' + r', & |r'| &\leq |\frac{n}{2}|. \end{aligned}$$

Ainsi,

$$x = (q + iq')y + (r + ir')y$$

et l'entier de Gauss $(r + ir')y$ est de norme inférieure à celle de y. □

L'anneau $\mathbf{Z}[i]$ est Euclidien ce qui a été obtenu dans le cas de l'anneau $\mathbf{Z}$ vaut pour $Z[i]$.

Théorème 4.2. *Soit m un entier de Gauss. Il existe $N(m)$ résidus modulo m et l'anneau quotient $\mathbf{Z}[i]/(m)$ est un corps si et seulement si m est irréductible.*

Démonstration. □

Pour profiter de ce théorème et construire des corps finis, il faut trouver des éléments irréductibles dans $\mathbf{Z}[i]$. Remarquons que 2 n'est pas irréductible puisque $(1+i)^2 = 2i$. Les unités de $\mathbf{Z}[i]$ sont les éléments de norme 1. Ainsi, $1+i$ est irréductible car en appliquant la norme à une factorisation $1+i = xy$,on obtient $2 = N(x)N(y)$ qui montre que x ou y est une unité. Cependant, l'anneau quotient $\mathbf{Z}[i]/(1 + i)$ est un corps à deux éléments isomorphe à $\mathbf{Z}/(2)$. Par contre, 3 est irréductible dans $\mathbf{Z}[i]$ et le corps $\mathbf{Z}[i]/(3)$ contient 9 éléments : il n'est pas isomorphe à un quotient de l'anneau $\mathbf{Z}$.

De la même façon, le lecteur montrera que $\mathbf{Z}[\sqrt{2}]$ est Euclidien mais qu'en général l'anneau $\mathbf{Z}[\omega]$ avec $\omega^2 \in \mathbf{Z}$ n'est pas toujours Euclidien.

Exercice 2. *Montrer que 2, 3, $1 + i\sqrt{5}$ et $1 - i\sqrt{5}$ sont irréductible non associés deux à deux dans $\mathbf{Z}[i\sqrt{5}]$. En déduire deux factorisation de 6, cet anneau est-il factoriel ? Euclidien ?*

5. Cardinalité

Soit A un anneau fini. L'ensemble des sous anneaux de A est stable par intersection et donc A possède un sous-anneau minimal qui est nécessairement isomrphe à un quotient $\mathbf{Z}/m\mathbf{Z}$ pour un certain entier m qui s'appelle la caractéristique de A celle d'un corps est un nombre premier.

Proposition 2. *L'ordre d'un corps fini est une puissance d'un nombre premier.*

Démonstration. Soit p la caractéristique d'un corps fini K. Le corps K contient un sous-corps isomorphe à $\mathbf{F}_p$ c'est donc un $\mathbf{F}_p$-espace vectoriel de dimension finie f et de cardinal p^f. □

6. Le théorème de Wederburn

Théorème 6.1. *Un corps fini est commutatif.*

7. Racine primitive

Proposition 3. *Soient K un corps commutatif et n un entier positif. Les solutions dans K de l'équation $X^n = 1$ forment un sous-groupe cyclique.*

Démonstration. C'est une conséquence du lemme qui suit. □

Lemme 1. *Soit G un groupe fini d'ordre n, G est cyclique si et seulement si pour tout diviseur d de n, G possède un et un seul sous-groupe d'ordre d.*

Démonstration. □

En particulier, un corps fini

8. Polynômes

L'anneau des polynôme $\mathbf{F}_p[X]$ possède une division Euclidienne. En procédant comme dans l'anneau $\mathbf{Z}$, nous obtenons un procédés de construction de corps finis.

Théorème 8.1. *Soit $\pi(X) \in \mathbf{F}_p[X]$ un polynôme de degré d. L'anneau quotient $\mathbf{F}_p[X]/(\pi(X))$ contient $q = p^d$ éléments c'est un corps si et seulement si $\pi(X)$ est irréductible.*

Démonstration. Il suffit de procéder comme dans la section 2. □

Proposition 4. *Soit K un corps fini de caractéristique p. Il existe un polynôme irréductible $\pi(X)$ tel que K soit isomorphe au quotient de $\mathbf{F}_p[X]$ par $\pi(X)$.*

9. Clotûre algébrique

Théorème 9.1. *Soit d un entier positif. Il existe un corps de Galois d'ordre p^d.*

Démonstration. Il suffit de prouver l'existence d'un polynôme irréductible de degré d. □

Théorème 9.2. *Deux corps de Galois sont isomorphes si et seulement si ils ont le même ordre.*

On sait construire une clôture algébrique $\bar{\mathbf{F}_p}$ de $\mathbf{F}_p$. Le groupe des racines $(q-1)$-ième de l'unité dans $\bar{\mathbf{F}_p}$ est cyclique d'ordre $q-1$ il en résulte que pour toute puissance q

Soit n un nombre entier positif. L'ensemble des entiers relatifs est muni d'une relation dite de congruence. L'entier x est congru à y modulo n si et seulement si n divise $y - x$, on écrit $x \equiv y \mod n$; c'est une relation d'équivalence compatible avec les lois d'addition et de multiplication. Un entier compris entre 0 ert $n-1$ est un résidu modulo n. Pour tout couple de résidus (x, y) on note $x \oplus y$ et $x \otimes y$ les résidus définis par :

$$x + y \equiv x \oplus y \mod n; \quad xy = x \otimes y \mod n;$$

L'ensemble des résidus modulo n muni de ces deux lois constitue un anneau fini, commutatif et unitaire ; généralement noté $\mathbf{Z}/n\mathbf{Z}$: c'est un anneau ‹‹quotient››.

Proposition 5. *$\mathbf{Z}/n\mathbf{Z}$ est un corps si et seulement si n est premier.*

Démonstration. $a \times b = 0$ si et seulement si ab est divisible par n. Si n est premier alors le lemme d'Euclide implique que n divise a ou b i.e. l'un des résidus est nul. Inversement, si n est composé alors il existe deux résidus non-nuls a et b dont le produit vaut 0. □

Il résulte de cette proposition que si n est premier alors le nombre de solutions de l'équation $x^d = 1$ est au plus d. Remarquez que l'équation $x^2 = 1$ possède 4 solutions dans $\mathbf{Z}/8\mathbf{Z}$!

Théorème 9.3. *L'ensemble des éléments inversibles de $\mathbf{Z}/n\mathbf{Z}$ constitue un groupe $(\mathbf{Z}/n\mathbf{Z})^\times$ commutatif*[1] *pour la loi multiplicative.*

Démonstration. C'est absolument évident ! □

Théorème 9.4 (Fermat)**.** *Soit n un entier positif. Les assertions suivantes sont équivalentes :*

(1) pour tout résidu non-nul a : $a^{n-1} \equiv 1 \mod n$

(2) n est premier.

Démonstration. Si n n'est pas premier, il existe un diviseur de zéro qui ne peut pas satisfaire (1). Si n est premier le groupe $(\mathbf{Z}/n\mathbf{Z})^\times$ est d'ordre $n-1$ et le théorème de Lagrange qui affirme que l'ordre d'un élément divise l'ordre du groupe permet de conclure. □

Théorème 9.5 (Wilson)**.** *Soit n un entier positif. Les assertions suivantes sont équivalentes :*

(1) $(n-1)! \equiv -1 \pmod n$

(2) n est premier.

Démonstration. Si n n'est pas premier alors le produit est nul. Si n est premier, dans le tous les éléments d'ordre supérieur à 2 apparaissent avec leur inverse. Le produit est donc égal au produit des éléments d'ordre 2, 1 et -1 si n est impair. □

10. Résidus Quadaratiques

Maintenant, n désigne un nombre premier impair. Certain éléments de $\mathbf{Z}/n\mathbf{Z}$ sont des carrés et d'autres pas. Un résidu non-nul a est dit résidu quadratique modulo n ou résidu non-quadratique modulo n suivant que l'équation : $X^2 = a$ possède ou pas des solutions dans $\mathbf{Z}/n\mathbf{Z}$. L'ensemble des premiers est noté $\mathcal{Q}$ et celui des seconds $\mathcal{N}$. Enfin, on définit le symbole de Legendre modulo n :

$$\left(\frac{a}{n}\right) = \begin{cases} +1, & a \in \mathcal{Q}; \\ 0, & \text{a=0}; \\ -1, & a \in \mathcal{N}. \end{cases} \tag{5}$$

1. Il faut savoir que ce groupe est cyclique, ce résultat est fondamental, mais la théorie des groupes nécessaire pour en faire la preuve déborde du cadre élémentaire de cette note.

Dans la suite, nous remplacerons cette notation historique par $\nu_n(a)$. Pout tout résidu a, $\nu_p(a)$ s'appelle le caractère quadratique de a modulo n.

Théorème 10.1 (Euler)**.** *Il y a autant de résidus quadratiques que de résidus non-quadratiques. L'ensemble des résidus quadratiques modulo n constitue un sous-groupe d'ordre $\frac{n-1}{2}$ de $(\mathbf{Z}/n\mathbf{Z})^\times$ et le symbole de Legendre vérifie :*

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

Démonstration. Le théorème de Fermat et factorisation

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

montre que chaque élément de $(\mathbf{Z}/n\mathbf{Z})^\times$ satisfait $x^{\frac{n-1}{2}} = 1$ ou (exclusif) $x^{\frac{n-1}{2}} = 1$. On en déduit que $\mathcal{Q}$ est l'ensemble des solutions $x^{\frac{n-1}{2}} = 1$ et que $\mathcal{N}$ celui de $x^{\frac{n-1}{2}} = -1$

□

En particulier, -1 est un carré modulo n si et seulement si $n \equiv 1 \mod 4$.

Exercice 3. *Utilisez le théorème de Wilson pour résoudre l'équation $X^2 = -1$ dans $\mathbf{Z}/n\mathbf{Z}$.*

Lemme 2 (Gauss)**.** *Soit a un résidu modulo n. Pour les $\frac{p-1}{2}$ premiers résidus non-nuls t, on note r_t le reste de la division à reste minimal de at par n. Montrez que :*

$$\prod_{t=1}^{\frac{p-1}{2}} \text{signe}(r_t) = \nu_n(a)$$

Exercice 4. *Utilisez le lemme de Gauss pour prouver que le caractère quadratique de 2 vaut :*

$$\nu_n(2) = \begin{cases} +1, & n = \pm 1 \mod 8; \\ -1, & n = \pm 1 \mod 8; \end{cases}$$

11. La loi de réciprocité quadratique

Soient p et q deux nombres premiers impairs. La loi de réciprocité quadratique énoncée par Legendre mais prouvée par Gauss affirme :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \epsilon(p,q) \tag{6}$$

où $\epsilon(p,q) = (-1)^{(p-1)(q-1)/4}$ vaut -1 si et seulement si p et q sont congrus à 3 modulo 4.

Il existe plus d'une centaine de preuves. La preuve de Reichardt, exposée dans [**?**], est assez remarquable : basée sur le lemme de Gauss, elle n'utilise absolument pas la notion d'extension algébrique. La démonstration proposée repose sur les sommes de Gauss et les congruences généralisées aux anneaux entiers cyclotomiques. Elle constitue une introduction à la théorie algébrique des nombres. Pour des approfondissement, voir incontournable ouvrage de P. Samuel [**?**].

Le notion de congruence se généralise à tous les sous-anneaux du corps des nombres complexes. Dans un tel anneau A, pour tout entier q, nous écrirons encore

$$x \equiv y \mod qA$$

pour exprimer que q divise la difference $x-y$. C'est une relation d'équivalence compatible avec les lois d'addition et de multiplication ce qui permet de définir la notion d'anneau résiduel : A/qA. Considérons l'anneau des entiers de Gauss $\mathbf{Z}[i]$, chaque éléments $z \in \mathbf{Z}[i]$ se sécompose d'une et une seule manière comme $z = a + ib$, où a et b sont deux entiers. Il en résulte que l'ensemble des nombres $a+ib$ en faisant varier les entiers a et b dans l'ensemble des résidus modulo q forme un système de représentant de $\mathbf{Z}[i]/q\mathbf{Z}[i]$ et donc que cette anneau contient q^2 éléments. Le lecteur profitera de l'occasion pour étudier les anneaux :

$$\mathbf{Z}[i]/2\mathbf{Z}[i], \quad \mathbf{Z}[i]/3\mathbf{Z}[i], \quad \mathbf{Z}[i]/5\mathbf{Z}[i]$$

Il remarquera que le premier anneau est ‹‹nilpotent››, que le troisième est ‹‹réduit›› et que le deuxième est un corps à 9 éléments, extension de degré 2 de $\mathbf{Z}/3\mathbf{Z}$, c'est un corps fini non premier : un ‹‹corps de Galois››.

Exercice 5. *Utiliser la division à reste minimal pour montrer que l'anneau des entiers de Gauss est Euclidien. Quelques soient A et $B \neq 0$ dans $\mathbf{Z}[i]$ il existe un et un seul couple $(Q, R) \in \mathbf{Z}[i] \times \mathbf{Z}[i]$ tels que :*

$$A = BQ + R, \quad N(R) < N(B),$$

où $N(a+ib) = a^2+b^2$ est la norme de $a+ib$. Déterminer toutes les utinités puis tous les irréductibles de $Z[i]$.

Proposition 6. *Soient p et q deux nombres premiers distincts. L'anneau des congruences modulo q de l'anneau $\mathbf{Z}[\zeta_p]$ est fini. Pour cette congruence l'entier p est inversible.*

Démonstration. En effet, ζ_p est racine de X^p-1 et donc l'anneau $\mathbf{Z}[\zeta_p]/q\mathbf{Z}[\zeta_p]$ possède au plus q^p éléments, et p inversible dans $\mathbf{Z}/q\mathbf{Z}$ demeure inversible dans $\mathbf{Z}[\zeta_p]/q\mathbf{Z}[\zeta_p]$. □

12. Caractères et Sommes de Gauss

Un homorphisme d'un groupe fini vers le groupe multiplicatif des nombres complexes est un caractère, en particulier $a \mapsto \nu_n(a)$ est un caractère du groupe $(\mathbf{Z}/n\mathbf{Z})^\times$. Il suit de la proposition précédente que la somme

$$\sum_{a \in (\mathbf{Z}/n\mathbf{Z})^\times} \nu_n(a) \tag{7}$$

est nulle. C'est une propriété générale des caractères de groupes. Par exemple, l'application $\mu\colon a \mapsto \zeta_p^a$ est un homomorphisme du groupe additif de $\mathbf{Z}/n\mathbf{Z}$, c'est un caractère additif canonique. Le lecteur n'aura pas de difficulté à vérifier que :

$$\sum_{a \in \mathbf{Z}/n\mathbf{Z}} \mu(a) = 0 \tag{8}$$

Pour tout résidu non-nul a, on définit la somme de Gauss :

$$g(a,n) = \sum_{x \in (\mathbf{Z}/n\mathbf{Z})^\times} \nu_n(a)\mu(a)$$

Cette somme est liée à la somme de Gauss quadratique $G(a,n)$ la relation $G(a,n) = 1 + \frac{1}{2}g(a,n)$. Elle est à l'avantage de faire apparaître le symbole de Legendre :

$$g(a,n) = \nu_n(a)g(1,n); \quad g(a,n)^* = \nu_n(-1)g(1,n). \tag{9}$$

Proposition 7. *Le module de la somme de Gauss $g(a,n)$ est égal à n, et*

$$g(a,n)^2 = \nu_n(-1)n.$$

Démonstration. Il faut faire le calcul direct du produit $g(a,n)g(a,n)^*$ et utiliser les relations (7) et (8). □

Voilà, nous sommes en mesure de faire une preuve de la loi de réciprocité quadradique à partir des sommes de Gauss et des anneaux cyclotomiques. Soient p et q deux premiers impairs et distincts, posons $A = \mathbf{Z}[\zeta_p]$. La divisibilité par q des coefficients binomiaux de rang q donne :

$$\begin{aligned} g(1,p)^q &\equiv g(q,p) \mod qA \\ &\equiv \nu_p(q)g(1,p) \mod qA \end{aligned} \tag{10}$$

Remarquons que $g(1,p)$ est inversible modulo q puisque son carré : $\pm p$ l'est. On peut simplifier :

$$g(1,p)^{q-1} \equiv \nu_p(q) \mod qA.$$

En élevant à la puissance $\frac{q-1}{2}$ l'égalité de la proposition (12), nous obtenons :

$$\left(g(a,p)^2\right)^{\frac{q-1}{2}} = \epsilon(p,q)p^{\frac{q-1}{2}} \equiv \epsilon(p,q)\nu_q(p) \equiv \nu_p(q) \mod qA$$

ce qui achève la preuve de la loi de réciprocité quadratique. Le lecteur familier avec les corps de Galois définira des sommes de Gauss dans un corps fini bien choisi pour simplifier cette démonstration, voir le petit livre d'arithmétique de Serre [**?**]. Une autre démonstration d' Eisenstein basée sur le lemme de Gauss y est proposée.

Exercice 6. *Utiliser la loi de réciprocité quadratique et les formules complémentaires pour écrire un algorithme* `Quadratique(a,p)` *qui calcule le caractère quadratique de a modulo p sachant que p est premier. Evaluer la complexité de votre algorithme !*