

Leçon 123 : Corps finis. Applications

[Cal-Per] : *Carnet de voyage en Algèbre*, Phillipe Caldero, Marie Peronnier

[Goz] : *Théorie de galois*, Ivan Gozard

[Per] : *Cours d'algèbre*, Daniel Perrin

[Sau-Ran] : *Cours de calcul formel. Corps finis, systèmes polynomiaux, applications*,

Phillipe Saux Picart, Eric Rannou

[Szp] : *Mathématiques Algèbre L3*, Aviva Szpirglas

[Ulm] : *Théorie des groupes*, Félix Ulmer

I Partie A - Construction et premières propriétés

I.1 Rappels rapides sur les extensions de corps [Goz]

■ **Déf 1 (Caractéristique) :**

■ **Prop 2 (Caractéristique d'un corps fini) :**

■ **Déf 3 (Corps premier, sous-corps premier) :**

■ **Ex 4 :** $\mathbb{Q}$ et $\mathbb{F}_p$

■ **Prop 5 (Sous-corps premiers) :**

■ **Prop 6 (Cardinal d'un corps fini) :**

■ **Ex 7 :** Exemples de corps qui ne peuvent exister.

■ **Déf 8 (Corps de rupture) :**

■ **Déf 9 (Corps de décomposition) :**

I.2 Construction des corps finis [Goz]

■ **Prop 10 (Frobenius) :**

■ **App 11 :** Racine p -ième.

■ **Thm 12 (Existence des corps finis) :**

■ **Rem 13 :** Construction des corps fini comme corps de rupture.

■ **Ex 14 :** $\mathbb{F}_4$, $\mathbb{F}_8$ et $\mathbb{F}_9$ [Annexe : Table de $\mathbb{F}_4$].

I.3 Structure des corps finis [Goz] [Ulm] [Szp]

■ **Prop 15 (Structure de $\mathbb{F}_q^\times$) :**

■ **Ex 16 :** Nombres de générateurs pour les $\mathbb{F}_p$, exemple de générateur pour $\mathbb{F}_{25}$

■ **Thm 17 (Élément primitif) :**

■ **Ex 18 :** Le faire pour $\mathbb{F}_9$

■ **Thm 19 (Sous-corps d'un corps fini) :**

■ **Ex 20 :** [Annexe : sous-corps de $\mathbb{F}_{2^{12}}$]

■ **Cor 21 :** Décomposition de $X^{p^n} - X$.

■ **Thm 22 (Structure du groupe des automorphismes) :**

II Partie B - Carrés [Goz] [Per]

II.1 Premières propriétés sur les carrés

■ **Déf 23 (Carrés de $\mathbb{F}_q$) :**

■ **Prop 24 (Cardinal de $\mathbb{F}_q^2$) :**

■ **Ex 25 :** Carrés de $\mathbb{F}_4$.

■ **Prop 26 (Caractérisation des carrés) :**

■ **Ex 27 :** Carrés de $\mathbb{F}_5$, carrés de $\mathbb{F}_9$ via le théorème de l'élément primitif.

■ **App 28 :** Il existe une infinité de nombres premiers de la forme $4k + 1$.

■ **Thm 29 (Première loi complémentaire) :**

■ **Prop 30 :** Dans un corps fini, tout élément est somme de deux carrés.

■ **App 31 (Classification des formes quadratiques) :**

II.2 Réciprocité quadratique [Sau-Ran]

■ **Déf 32 (Somme de Gauss) :**

■ **Prop 33 (Lemme somme de Gauss) :**

| **Déf 34 (Symbole de Legendre, résidu quadratique) :**

| **Ex 35 :** Résidus quadratiques dans $\mathbb{F}_7$.

| **Prop 36 :** On a $\left(\frac{x}{p}\right) = x^{(p-1)/2}$ dans $\mathbb{F}_p$.

| **Thm 37 (Réciprocité quadratique) :**

App 38 (Calcul du symbole de Legendre) : Voir [Goz].

|  **Dév 39 (Nombres de Mersennes) :**

III Partie C - Polynômes

III.1 Irréductibilité sur $\mathbb{F}_p$ [Goz] [Per] [Ulm]

| **Thm 40 (Construction de $\mathbb{F}_q$ comme corps de rupture) :**

App 41 : Il existe une infinité de polynômes irréductibles de degré n dans $\mathbb{F}_p$.

| **Thm 42 (Facteurs irréductibles de $X^{pn} - X$) :**

| **Thm 43 (Nombre de polynômes irréductibles) :**

| **Ex 44 :** Voir [Goz].

| **Thm 45 (Berlekamp) :**

| **Ex 46 :** Voir [Ulm]

| **Prop 47 (Irréductibilité et racines) :**

| **Ex 48 :**
Voir [Per].

III.2 Irréductibilité sur $\mathbb{Z}$ et $\mathbb{Q}$ [Per]

| **Thm 49 (Eisenstein) :**

App 50 : Irréductibilité de Φ_p , degré d'une extension cyclotomique.

| **Thm 51 (Réduction) :**

| **Ex 52 :** Voir [Per].

| **Contre-Ex 53 :** $X^4 + 1$ est irréductible sur $\mathbb{Z}$ et $\mathbb{Q}$, mais sur aucun $\mathbb{F}_p$.

IV Partie D - Matrices sur un corps fini [Cal-Per]

| **Prop 54 (Lemme de Fitting) :**

App 55 (Dénombrement du cône nilpotent) :

|  **Dév 56 (Proba sur des matrices) :**

| **Prop 57 (Dénombrement des matrices diagonalisables) :**