Université d'Évry Val d'Essonne 2011-2012

M54 algèbre et arithmétique 2

Squelette de cours

Introduction : structures algébriques

Définition 1. On appelle monoïde un ensemble muni d'une loi associative admettant un élément neutre.

Définition 2. On appelle groupe un monoïde dans lequel tout élément possède un symétrique.

Le symétrique est appelé inverse si le groupe est multiplicatif, opposé s'il est additif, et réciproque si les éléments du groupes sont des fonctions.

Un groupe est dit abélien si sa loi est commutative.

Définition 3. On appelle anneau un ensemble A muni de deux lois $+$ et $\cdot$ telles que
- $(A, +)$ est un groupe abélien ;
- $(A, \cdot)$ est un monoïde ;
- la multiplication est distributive sur l'addition.

On dit que l'anneau est commutatif si sa multiplication l'est.

Définition 4. Un corps est un anneau commutatif A tel que $(A \setminus \{0\}, \cdot)$ est un groupe.

Définition 5. On appelle module sur un anneau A un ensemble M muni d'une loi interne (addition) et d'une multiplication externe par les éléments de A telles que $(M, +)$ est un groupe abélien et, pour tous x, y dans M et λ, μ dans A, on a

1. $1 \cdot x = x$;
2. $(\lambda\mu) \cdot x = \lambda \cdot (\mu \cdot x)$;
3. $(\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x$;
4. $\lambda(x + y) = \lambda x + \lambda y$.

Si A est un corps, on parle d'espace vectoriel.

Définition 6. On appelle algèbre sur un corps K un anneau A qui est également muni d'une structure de K-espace vectoriel telle que, pour tous λ dans K et x, y dans A, on a $(\lambda x)y = \lambda(xy)$.

Remarque 7. Une autre façon de voir les choses est que :
- dans un monoïde, il y a une opération (l'addition par exemple) ;
- dans un groupe, il y en a deux : l'addition et la soustraction (par exemple) ;
- dans un anneau, trois : addition, soustraction, multiplication ;
- dans un corps, quatre : addition, soustraction, multiplication, division.

Remarque 8. À partir de maintenant, **tous les anneaux sont supposés commutatifs** sauf précision contraire !

I Anneaux, corps : généralités

I.1 Opérations et propriétés de base

Exemple I.1.1. Quelques opérations de base sur les anneaux.

1. Si A est un anneau et E un ensemble, l'ensemble des fonctions de E dans A est un anneau.
2. Si A est un anneau et X une variable, l'ensemble $A[X]$ des polynômes en une variable à coefficients dans A est un anneau.
3. Si A et B sont deux anneaux, $A \times B$ est un anneau.
4. Si A est un anneau, l'ensemble $M_n(A)$ des matrices carrées de taille n à coefficients dans A est un anneau *non commutatif*.

Définition I.1.2. Soient A un anneau et $x \in A$, on dit que x est :
- inversible (ou que x est une unité de A) s'il existe $y \in A$ tel que $xy = 1$;
- simplifiable si, pour tous y et z, on a $xy = xz \implies y = z$;
- diviseur de zéro s'il existe y tel que $xy = 0$;

Proposition I.1.3. Les éléments inversibles sont simplifiables.

Un élément est simplifiable si et seulement si il n'est pas diviseur de zéro.

Définition I.1.4. On note $A^\times$ l'ensemble des éléments inversible de A ; c'est un groupe pour la multiplication, appelé groupe multiplicatif de A.

Définition I.1.5. On dit qu'un anneau est intègre s'il n'est pas réduit à 0 et que tous les éléments non nuls sont simplifiables.

Proposition I.1.6. Les corps sont des anneaux intègres.

Notation I.1.7. Soit $n \in \mathbf{N}$; on note $x^n = \underbrace{x \cdot \cdots \cdot x}_{n \text{ fois}}$.

Si de plus x est inversible, on note x^{-1} son inverse, et $x^{-n} = (x^{-1})^n$.

Définition I.1.8. On dit que x est nilpotent s'il existe $n \in \mathbf{N}$ tel que $x^n = 0$.

On dit que x est idempotent si $x^2 = x$.

Proposition I.1.9. Les éléments nilpotents sont diviseurs de zéro ; les éléments idempotents différents de 1 sont diviseurs de zéro.

I.2 Morphismes

Définition I.2.1. Soient A et B deux anneaux ; un morphisme d'anneaux de A dans B est une application de A dans B qui est un morphisme de groupes de $(A, +)$ dans $(B, +)$ et un morphisme de monoïdes de $(A, \cdot)$ dans $(B, \cdot)$.

On appelle morphisme de corps un morphisme d'anneaux entre deux corps.

Critère I.2.2. Une application $f \colon A \to B$ est un morphisme si :

1. $f(a + b) = f(a) + f(b)$;

2. $f(a \cdot b) = f(a) \cdot f(b)$;
3. $f(1) = 1$.

Proposition I.2.3. La composée de deux morphismes est un morphisme.

Proposition I.2.4. Si f est un morphisme bijectif, sa réciproque est un morphisme.

Définition I.2.5. On appelle :
- endomorphisme un morphisme d'un anneau dans lui-même ;
- isomorphisme un morphisme bijectif ;
- automorphisme un endomorphisme bijectif.

I.3 Sous-anneaux

Définition I.3.1. Soit A un anneau et $B \subset A$ un sous-ensemble ; on dit que B est un sous-anneau de A si c'est un anneau pour les opérations induites par celles de A.

Critère I.3.2. B est un sous-anneau si :

1. $1 \in B$;
2. pour tous x et y dans B, on a $x - y \in B$ et $xy \in B$.

Définition I.3.3. Soit K un corps et $B \subset K$ un sous-ensemble ; on dit que B est un sous-corps de K si c'est un corps pour les opérations induites par celles de K.

Critère I.3.4. B est un sous-corps si :

1. $B \neq \emptyset$;
2. pour tous x et y dans B, on a $x - y \in B$ et $xy^{-1} \in B$.

Proposition I.3.5. Soient B_1 et B_2 deux sous-anneaux de A, alors $B_1 \cap B_2$ est un sous-anneau de A.

Remarque I.3.6. En général, l'union, ou même la somme, de deux sous-anneaux, n'est pas un sous-anneau.

Définition I.3.7. Soit $S \subset A$ un sous-ensemble ; on appelle sous-anneau engendré par S le plus petit sous-anneau de A qui contient S.

Critère I.3.8. B est le sous-anneau engendré par S si :

1. B est un sous-anneau contenant S ;
2. si B' est aussi un sous-anneau contenant S, on a $B \subset B'$.

Définition I.3.9. Soient E et F deux ensembles et $f\colon E \to F$ une application. Soient de plus $E_1 \subset E$ et $F_1 \subset F$, on note :

$$f(E_1) = \{y \in F \text{ tq } \exists x \in E,\ y = f(x)\}$$
$$f^{-1}(F_1) = \{x \in E \text{ tq } f(x) \in F_1\}$$

Définition I.3.10. Soit $f\colon A \to B$ un morphisme d'anneaux, on note $\operatorname{im} f = f(A)$ et $\ker f = f^{-1}(\{0\})$.

Proposition I.3.11. Soit $f\colon A \to B$ un morphisme d'anneaux, A_1 un sous-anneau de A et B_1 un sous-anneau de B ; alors $f(A_1)$ est un sous-anneau de B et $f^{-1}(B_1)$ un sous-anneau de A.

Corollaire I.3.12. $\operatorname{im} f$ est un sous-anneau de B.

Remarque I.3.13. Si $B \neq \{0\}$, alors $\{0\}$ n'est pas un sous-anneau de B et $\ker f$ n'est en général pas un sous-anneau de A.

I.4 Idéaux

Définition I.4.1. On appelle idéal d'un anneau A un sous-groupe de $(A, +)$ stable par multiplication par les éléments de A.

Critère I.4.2. $I \subset A$ est un idéal si :

1. $0 \in I$;
2. pour tous x, y dans I et $a \in A$, on a $ax - y \in I$.

Proposition I.4.3. Soit $f\colon A \to B$ un morphisme d'anneaux, alors $\ker f$ est un idéal de A.

Définition I.4.4. Soit $a \in A$; on appelle idéal principal engendré par a et on note (a) l'ensemble des multiples de a dans A ; c'est un idéal de A, qui est égal à A si et seulement si $a \in A^\times$.

Proposition I.4.5. Un anneau est un corps si et seulement si ses seuls idéaux sont $\{0\}$ et lui-même.

Remarque I.4.6. Plus généralement, un idéal qui contient un élément inversible est égal à l'anneau entier.

Proposition I.4.7. L'intersection de deux idéaux est un idéal.

Définition I.4.8. Soit $X \subset A$ un sous-ensemble ; on appelle idéal engendré par X le plus petit idéal de A qui contient X.

Proposition I.4.9. Si $X = \{x_1, \ldots, x_n\}$ l'idéal engendré par X est noté $(x_1, \ldots, x_n)$; c'est l'ensemble des combinaisons linéaires $a_1x_1 + \cdots + a_nx_n$.

Remarque I.4.10. L'union de deux idéaux n'est en général pas un idéal.

Proposition I.4.11. Soient I et J deux idéaux, alors l'ensemble

$$I + J = \{x + y \text{ avec } x \in I \text{ et } y \in J\}$$

est un idéal.

Définition I.4.12. Soient I et J deux idéaux, on note IJ l'idéal *engendré* par les produits xy avec $x \in I$ et $y \in J$.

Proposition I.4.13. $IJ \subset I \cap J$.

Proposition I.4.14. L'ensemble des éléments nilpotents de A est un idéal de A.

Proposition I.4.15. Soit $f\colon A \to B$ un morphisme et J un idéal de B ; alors $f^{-1}(J)$ est un idéal de A.

I.5 Quotients

Théorème I.5.1. Soit A un anneau et I un idéal de A.

1. La relation $\sim_I$ définie par
$$x \sim_I y \Leftrightarrow x - y \in I$$
est une relation d'équivalence.
2. Pour tout $x \in A$, la classe de x est $cl_I(x) = x + I$.
3. Cette relation est compatible avec les opérations :
$$x \sim_I y \text{ et } x' \sim_I y' \implies (x + x') \sim_I (y + y') \text{ et } (x + x') \sim_I (y + y')$$
4. L'ensemble quotient muni des opérations induites est un anneau, et cl_I est un morphisme.

Définition I.5.2. On note A/I le quotient, et le morphisme cl_I est appelé surjection canonique.

Proposition I.5.3. Soit $f\colon A \to B$ un morphisme et I un idéal de A. Si $I \subset \ker f$, alors il existe un unique morphisme $\tilde{f}\colon A/I \to B$ tel que $f = \tilde{f} \circ cl_I$.

Théorème I.5.4. Soit $f\colon A \to B$ un morphisme, alors
$$A/\ker f \approx \operatorname{im} f$$
Plus précisément, on a $f = \iota \circ \tilde{f} \circ cl_{\ker f}$ où $cl_{\ker f}$ est surjectif, $\tilde{f}$ est un isomorphisme, et ι est injectif.

II Arithmétique dans Z et les anneaux euclidiens

II.1 Rappels : Euclide et Bézout

Définition II.1.1 (Algorithme d'Euclide)**.** Soit a et b deux entiers, on définit une suite d'entiers par récurrence en partant de $r_0 = a$ et $r_1 = b$ puis r_{i+1} est le reste de la division euclidienne de r_{i-1} par r_i, jusqu'à avoir $r_{i+1} = 0$; on note $n = i$ le dernier indice.

Proposition II.1.2. On a $r_n = \operatorname{pgcd}(a, b)$.

Définition II.1.3. On appelle relation de Bézout entre a et b une relation de la forme $au + bv = PGCD(a, b)$ avec u et v entiers.

Proposition II.1.4. Les relations de Bézout existent toujours ; elles s'obtiennent en « remontant » l'algorithme d'Euclide.

II.2 Inversibles de $\mathbf{Z}/n\mathbf{Z}$ et équation $ax = b \mod n$

Théorème II.2.1. $a \in (\mathbf{Z}/n\mathbf{Z})^\times \Leftrightarrow \operatorname{pgcd}(a, n) = 1$

Corollaire II.2.2. $\mathbf{Z}/n\mathbf{Z}$ est un corps si et seulement si n est premier.

Méthode II.2.3. Pour calculer l'inverse de a modulo n, on calcule une relation de Bézout entre a et n.

Méthode II.2.4. Pour résoudre $ax = b \mod n$, on pose $d = \text{pgcd}(a, n)$:
- si $d \nmid b$ il n'y a pas de solution ;
- si $d \mid b$ on simplifie par d (y compris n) et on arrive au cas suivant :
- si $d = 1$ alors a est inversible et la solution est $x = b \cdot a^{-1} \mod n$.

II.3 Théorème chinois et systèmes de congruences

Théorème II.3.1. Soient n et m deux entiers premiers entre eux, alors

$$\mathbf{Z}/mn\mathbf{Z} \approx (\mathbf{Z}/m\mathbf{Z}) \times (\mathbf{Z}/n\mathbf{Z})$$

Théorème II.3.2. Soient n et m deux entiers quelconques, et

$$\phi \colon \mathbf{Z} \to (\mathbf{Z}/n\mathbf{Z}) \times (\mathbf{Z}/m\mathbf{Z})$$

alors $\ker \phi = (\text{pgcd}(n, m))$ et $\text{im}\, \phi = \{(a, b) \text{ tq } a = b \mod \text{pgcd}(n, m)\}$.

Méthode II.3.3. Pour résoudre un système de congruences

$$\begin{cases} x = a \mod n \\ x = b \mod m \end{cases}$$

on calcule $d = \text{pgcd}(n, m)$ puis
- si $a \neq b \mod d$ il n'y a pas de solution ;
- sinon, on a calcule une relation de Bézout entre n/d et m/d, notons-la $un/d + vm/d = 1$; on pose $x_0 = bun/d + avm/d$; les solutions sont $x = x_0 \mod nm/d$.

II.4 Le groupe $(\mathbf{Z}/n\mathbf{Z})^\times$

Proposition II.4.1 (Rappel : théorème de Lagrange)**.** Soit G un groupe multiplicatif fini d'ordre n, alors pour tout $x \in G$ on a $x^n = 1$.

Autrement dit, l'ordre de tout élément divise l'ordre du groupe.

Théorème II.4.2 (Petit théorème de Fermat)**.** Soit p un nombre premier et a un entier non multiple de p, alors $a^{p-1} = 1 \mod p$.

Corollaire II.4.3. Soit p premier, alors pour tout a on a $a^p = a \mod p$.

Définition II.4.4. On appelle indicatrice d'Euler la fonction

$$\begin{aligned} \phi \colon \mathbf{N} &\to \mathbf{N} \\ n &\mapsto \text{Card}(\mathbf{Z}/n\mathbf{Z})^\times \end{aligned}$$

Théorème II.4.5 (Théorème d'Euler)**.** Si a et n sont premiers entre eux, alors $a^{\phi(n)} = 1 \mod n$.

Lemme II.4.6. Si p est premier, on a $\phi(p) = p - 1$.

Lemme II.4.7. Si p est premier et $r \in \mathbf{N}$, on a $\phi(p^r) = p^{r-1}(p - 1)$.

Lemme II.4.8. Soient n et m deux entier premiers entre eux, alors $\phi(mn) = \phi(m)\phi(n)$.

Proposition II.4.9. Soit n un entier et $p_1^{r_1} \cdots p_q^{r_q}$ sa décomposition en facteurs premiers, alors $\phi(n) = p_1^{r_1-1}(p_1 - 1) \cdots p_q^{r_q-1}(p_q - q)$.

II.5 Interlude : notions de cryptographie

Définition II.5.1. On appelle cryptosystème la donnée de :
- un ensemble M des messages en clair possibles ;
- un ensemble C des messages chiffrés possibles ;
- une fonction $E\colon M \to C$ de chiffrement ;
- une fonction $D\colon C \to M$ de déchiffrement ;

telles que $D \circ E = \mathbf{Id}_M$.

En pratique, les fonctions E et D dépendent de paramètres appelés clés, dont certains sont tenus secrets, de sorte qu'il est pratiquement impossible de calculer D sans connaître la clé secrète.

Le principe de Kerckhoffs (1883) énonce que dans un bon cryptosystème, la sécurité ne doit reposer que sur le caractère secret de la clé ; tous les autres éléments du cryptosystème sont publics ; la clé doit pouvoir être changée facilement.

Définition II.5.2. Un cryptosystème est dit symétrique si les deux fonctions E et D dépendent d'une même clé (secrète).

Un cryptosystème est dit asymétrique si E dépend d'une certaine clé P, dit clé de chiffrement ou clé publique, alors que D dépend d'une autre clé S, dite clé de déchiffrement ou clé secrète.

II.6 Le cryptosystème RSA

Méthode II.6.1 (Fabrication d'une paire de clé)**.** Alice choisit deux grands nombres premiers distincts p et q, tenus secrets. Elle calcule $n = pq$ et $\phi(n) = (p-1)(q-1)$, puis choisit e un entier premier à $\phi(n)$ et calcule l'inverse d de e modulo $\phi(n)$.

Sa clé publique est $P = (e, n)$ et sa clé secrète est $S = d$.

Définition II.6.2. Dans le cryptosystème RSA, on a
- $M = C = \mathbf{Z}/n\mathbf{Z}$;
- $E(m) = m^e \mod n$;
- $D(c) = c^d \mod n$.

Proposition II.6.3. Si la paire de clé a été fabriqué comme ci-dessus, $D \circ E$ est l'identité.

II.7 Anneaux euclidiens, principaux

Définition II.7.1. Soit A un anneau intègre. On dit que A est euclidien s'il existe une fonction (appelée stathme) $N\colon A \setminus \{0\} \to \mathbf{N}$ telle que, pour tous $a \in A$ et $b \in A \setminus \{0\}$, il existe $q \in A$ et $r \in A$ tels que :

$$a = bq + r \quad \text{et } r = 0 \text{ ou } N(r) < N(b)$$

Définition II.7.2. On dit qu'un anneau est principal s'il est intègre et que tous ses idéaux sont principaux.

Théorème II.7.3. Les anneaux euclidiens sont principaux.

II.8 Arithmétique dans les anneaux principaux

Proposition II.8.1. Soient a et b deux éléments d'un anneau A quelconque. Alors $(a) \subset (b) \Leftrightarrow b \mid a$.

Proposition II.8.2. Soit A un anneau principal et a et b deux éléments, alors

1. $(a) \cap (b) = (\mathrm{ppcm}(a, b))$;
2. $(a) + (b) = (\mathrm{pgcd}(a, b))$;
3. $(a) \cdot (b) = (ab)$.

II.9 Idéaux premiers et maximaux

Définition II.9.1. Soit I un idéal d'un anneau A ; on dit que I est premier si, pour tous a, b dans A, on a

$$ab \in I \implies a \in I \text{ ou } b \in I$$

Proposition II.9.2. Les idéaux premiers de $\mathbf{Z}$ sont (0) et les idéaux (p) où p est un nombre premier.

Proposition II.9.3. I est premier si et seulement si A/I est intègre.

Définition II.9.4. Soit I un idéal d'un anneau A ; on dit que I est maximal si $I \neq A$ et si, pour tout idéal J contenant I, on a $J = I$ ou $J = A$.

Proposition II.9.5. Les idéaux maximaux de $\mathbf{Z}$ sont les idéaux (p) où p est un nombre premier.

Proposition II.9.6. I est maximal si et seulement si A/I est un corps.

Corollaire II.9.7. Les idéaux maximaux sont premiers.

II.10 Anneaux factoriels

Définition II.10.1. On dit que deux éléments a et b d'un anneau A sont associés s'il existe $u \in A^\times$ tel que $a = ub$.

Proposition II.10.2. Dans un anneau intègre, a et b sont associés si et seulement si $(a) = (b)$.

Définition II.10.3. Soit a un élément d'un anneau A, on dit que a est irréductible s'il n'est pas inversible et si $a = bc$ implique que b ou c est inversible (et que l'autre est associé à a, donc).

Proposition II.10.4. Dans $\mathbf{Z}$ les irréductibles sont les nombres premiers et leurs opposés.

Lemme II.10.5. Soit p un élément irréductible d'un anneau principal A, alors

$$p \mid ab \implies p \mid a \text{ ou } p \mid b$$

Corollaire II.10.6. Soit p un élément non nul d'un anneau principal, alors les trois propositions suivantes sont équivalentes :

(i) p est irréductible ;

(ii) (p) est premier ;

(iii) (p) est maximal.

Définition II.10.7. On dit qu'un anneau intègre A est factoriel si tous ses éléments non nuls s'écrivent de façon essentiellement unique sous la forme

$$u \cdot p_1^{r_1} \cdots p_n^{r_n}$$

avec u inversible, p_i irréductible et $r_i \in \mathbf{N}$.

Proposition II.10.8. Soit A un anneau factoriel et p un élément irréductible, alors

$$p \mid ab \implies p \mid a \text{ ou } p \mid b$$

Théorème II.10.9. Les anneaux principaux sont factoriels.

Lemme II.10.10. Dans un anneaux quelconque, soit $(I_n)_n$ une suite croissante d'idéaux (c'est-à-dire $I_i \subset I_{i+1}$), alors leur union $\cup_{n\in N} I_n$ est encore un idéal.

Lemme II.10.11. Dans un anneau principal, tout suite croissante d'idéaux $(I_n)_n$ est stationnaire, c'est-à-dire qu'il existe $N \in \mathbf{N}$ tel que $I_i = I_N$ pour tout $i \geqslant N$.

Théorème II.10.12 (admis)**.** Si A est factoriel, alors $A[X]$ aussi.

III Anneaux de polynômes, corps finis et applications

Dans toute cette partie, K désigne un corps quelconque.

III.1 Généralités

Proposition III.1.1. $K[X]$ est une K-algèbre intègre et $K[X]^\times = K^\times$.

Proposition III.1.2. $K[X]$ est un anneau euclidien avec pour stathme le degré.

Corollaire III.1.3. $K[X]$ est principal, donc factoriel. En particulier, la proposition II.8.2 s'applique, et il existe toujours une relation de Bézout entre deux polynômes quelconques.

Remarque III.1.4. C'est faux si K n'est pas un corps.

Remarque III.1.5. Dans la décomposition d'un polynôme en produit d'irréductibles, on peut de plus exiger que ces derniers soient unitaires : la décomposition est alors unique à l'ordre près.

III.2 Irréductibilité et racines

Définition III.2.1. Soit $P \in K[X]$ et $a \in K$; on dit que a est une racine de P si $P(a) = 0$.

Proposition III.2.2. a est une racine de P si et seulement si $X - a$ divise P.

Remarque III.2.3. Un polynôme de degré 1 admet toujours exactement une racine.

Critère III.2.4 (irréductibilité en petit dégrés)**.**
- Les polynômes de degré 0 ne sont jamais irréductibles.
- Les polynômes de degré 1 sont toujours irréductibles.
- Un polynôme de degré 2 ou 3 est irréductible si et seulement si il n'admet pas de racines.
- Un polynôme de degré 4 ou 5 est irréductible si et seulement si il n'admet pas de racines *et* n'est divisible par aucun polynôme irréductible de degré 2.

Remarque III.2.5. Les polynômes de degré 1 sont les seuls polynômes irréductibles à avoir des racines.

Lemme III.2.6. Soient a et b deux éléments de K distincts ; alors $X - a$ et $x - b$ sont premiers entre eux. Plus généralement, si $a_1, \dots a_n$ sont des éléments distincts, alors $X - a_1$ est premier avec $\prod_{i=2}^{n}(X - a_i)$.

Corollaire III.2.7. Soient $a_1, \dots, a_n$ des racines distinctes d'un polynôme P, alors $(X - a_1) \cdots (X - a_n)$ divise P.

Proposition III.2.8. Un polynôme non nul de degré n admet au plus n racines distinctes.

III.3 Quotients, extensions de corps

Proposition III.3.1. Soit $f \colon K \to A$ un morphisme d'anneaux, alors la loi définie par $\lambda \cdot a = f(\lambda)a$ pour $\lambda \in K$ et $a \in A$ définit une structure de K-algèbre sur A.

Proposition III.3.2. Soit $P \in K[X]\backslash\{0\}$, alors le quotient $K[X]/(P)$ est une K-algèbre de dimension $\deg P$; plus précisément, si l'on note α la classe de X dans le quotient, alors $1, \alpha, \alpha^2, \dots, \alpha^{\deg P - 1}$ est une base du quotient en tant que K-espace vectoriel.

Proposition III.3.3. $K[X]/(P)$ est un corps si et seulement si P est irréductible.

Proposition III.3.4. Soit $f \colon K \to A$ un morphisme d'un corps dans un anneau non nul ; alors f est injectif.

Définition III.3.5. Soient K et L deux corps ; on dit que L est une extension de K s'il contient K ou, plus généralement, s'il existe un morphisme (nécessairement injectif) de K dans L (qui contient alors un sous-corps isomorphe à K).

Corollaire III.3.6. Si $P \in K[X]$ est irréductible, $K[X]/(P)$ est une extension de K.

III.4 Caractéristique

Définition III.4.1. Soit A un anneau et $f\colon \mathbf{Z} \to A$ l'unique morphisme ; il existe un unique $n \in \mathbf{N}$ tel que $\ker f = (n)$: cet entier est appelé la caractéristique de A et noté $\operatorname{car} A$.

Critère III.4.2. La caractéristique est le plus petit entier n tel que $\underbrace{1 + \cdots + 1}_{n \text{ fois}} = 0$, s'il en existe ; sinon, c'est 0.

Proposition III.4.3. Un anneau est de caractéristique n si et seulement si il contient un sous-anneau isomorphe à $\mathbf{Z}/n\mathbf{Z}$.

Corollaire III.4.4. Soit L une extension de K, alors $\operatorname{car} K = \operatorname{car} L$.

Proposition III.4.5. La caractéristique d'un anneau intègre (et en particulier, d'un corps) est soit 0 soit un nombre premier.

III.5 Corps finis

Proposition III.5.1. Soit F un corps fini, alors il existe un nombre premier $p = \operatorname{car} F$ et un entier n tel que $\operatorname{Card} F = p^n$.

Théorème III.5.2 (admis)**.** Le groupe multiplicatif d'un corps fini est cyclique.

Proposition III.5.3. Soit F un corps fini et $p = \operatorname{car} F$. Alors il existe un polynôme irréductible $P \in \mathbf{F}_p[X]$ tel que $F = \mathbf{F}_p[X]/(P)$.

Proposition III.5.4 (admise)**.** Pour tout nombre premier p et tout entier $n \geqslant 1$, il existe dans $\mathbf{F}_p[X]$ au moins un polynôme irréductible de degré n.

Théorème III.5.5. Soit q un entier ; il existe un corps à q éléments si et seulement si $q = p^n$ avec p premier et $n \in \mathbf{N}$.

Théorème III.5.6 (admis)**.** Soient F et F' deux corps finis de même cardinal ; alors ils sont isomorphes. En conséquence, on note $\mathbf{F}_q$ « le » corps à q éléments.

Proposition III.5.7 (partiellement admise)**.** Soient $\mathbf{F}_q$ et $\mathbf{F}_{q'}$ deux corps finis ; il existe un morphisme de $\mathbf{F}_q$ dans $\mathbf{F}'_q$ si et seulement si q' est une puissance de q.

Proposition III.5.8. Soit F un corps de caractéristique p. Alors $(a+b)^p = a^p + b^p$.

Définition III.5.9. Dans un corps de caractéristique p, l'application $x \mapsto x^p$ est un automorphisme, appelé morphisme de Frobenius.

Théorème III.5.10 (admis)**.** Le groupe $\operatorname{Aut} \mathbf{F}_q$ est cyclique et engendré par le morphisme de Frobenius.

III.6 Problème du log discret

Définition III.6.1. Soit G un groupe multiplicatif, cyclique, d'ordre N, et g un générateur de G. L'application

$$\begin{aligned} \mathbf{Z}/N\mathbf{Z} &\to G \\ n &\mapsto g^n \end{aligned}$$

est un isomorphisme appelé exponentielle de base g. Son morphisme réciproque est appelé logarithme discret de base g.

Remarque III.6.2. Lorsque $G = \mathbf{F}_q^\times$ (où q possède certaines propriétés) le logarithme discret est très long à calculer. On ne connaît pas de méthode sensiblement plus performante que de calculer les puissances successives de g jusqu'à obtenir le résultat voulu.

Remarque III.6.3. L'exponentielle se calcule rapidement en utilisant l'écriture en base 2 de l'exposant (méthode dite d'exponentiation rapide).

III.7 Protocole de Diffie-Hellman

Définition III.7.1. Le but pour Alice et Bob est de construire ensemble, publiquement, un élément qu'ils seront les seuls à connaître, appelé secret partagé.

1. Alice et Bob se mettent d'accord sur un corps $\mathbf{F}_q$ et un générateur g de $\mathbf{F}_q^\times$.
2. Alice choisit en secret un entier $a \in \{2, q-3\}$ et Bob choisit de même un entier b.
3. Alice calcule g^a et envoie de résultat à Bob, qui de son côté calcule g^b et envoie de résultat à Alice.
4. Alice calcule $(g^b)^a$ et Bob calcule $(g^a)^b$.

Leur secret partagé est g^{ab}.

Remarque III.7.2. Il est conjecturé (mais pas prouvé) que calculer g^{ab} en connaissant seulement g^a et g^b est aussi difficile que de trouver a à partir de g^a, c'est-à-dire de calculer un log discret.

III.8 Cryptosystème El Gamal

Définition III.8.1 (fabrication d'une paire de clés)**.** Alice choisit un corps fini $\mathbf{F}_q$ et un générateur g de $\mathbf{F}_q^\times$, puis un entier $a \in \{2, \dots, q-3\}$, et calcule g^a. Sa clé publique est $(\mathbf{F}_q, g, g^a)$; sa clé secrète est a.

Définition III.8.2. Le cryptosystème El Gamal est défini par
- $M = \mathbf{F}_q^\times$;
- $C = \mathbf{F}_q^\times \times \mathbf{F}_q^\times$;
- $E_x(m) = (g^x, mg^{ax})$ où $x \in \{2, \dots, q-3\}$ est choisi au hasard ;
- $D(c_1, c_2) = c_2 \cdot c_1^{-a}$.