MA 435 Paris Tech Shanghai : Introduction aux corps finis

Table des matières

Le cours MA 435 est un cours fondamental d'algèbre dont le but est d'introduire les structures algébriques de base, à travers des exemples et l'étude de leurs propriétés. Parmi ces structures algébriques on retrouve d'un côté des objets arithmétiques déjà connus (les nombres entiers ou rationnels, des congruences) et de l'autre côté on introduit le formalisme nécessaire pour étudier des structures plus générales, ce qui est fondamental pour des cours avancés en algèbre, ainsi que pour des applications à la théorie des codes et à la cryptographie. En particulier, le standard actuel de cryptographie à clé secrète (Advanced Encryption System AES) repose sur l'arithmétique dans les anneaux de polynômes et dans les corps finis.

La rédaction de ces notes suit un cours de David Harari, ainsi que les livres "Algèbre" de Xavier Gourdon, "Cours d'algèbre" de Daniel Perrin, "Arithmétique" de Marc Hindry et d'autres.

Chapitre 1

Groupes

1.1 Relations d'équivalence, structures quotient

Soit E un ensemble (non vide), par exemple $E = \mathbb{Z}$ l'ensemble des nombres entiers. Une *relation d'équivalence* sur E permet d'identifier certains éléments de E. Par exemple, si l'on s'intéresse à la parité de nombres entiers, on peut dire que $a \sim b$ pour deux entiers a et b si $2|a-b$. On voit donc que l'on distingue certains couples d'entiers (a, b) (ceux dont la différence est paire).

Définition 1.1.1. Soient E et F deux ensembles. Le *produit cartésien* de E et F noté $E \times F$ est l'ensemble des couples (x, y) où $x \in E$ et $y \in F$:

$$E \times F = \{(x, y) \,|\, x \in E, y \in F\}.$$

Définition 1.1.2. Une relation binaire entre deux ensembles E et F est une partie (un sous-ensemble) $\mathcal{R}$ du produit cartesien $E \times F$. Pour $x \in E$ et $y \in F$ on note $x\mathcal{R}y$ ou $x \sim_{\mathcal{R}} y$ (où même simplement $x \sim y$) si $(x, y) \in \mathcal{R}$. Si $E = F$ on dit qu'on a une relation binaire sur E.

Exemples

1. si $f : E \to F$ une application entre deux ensembles, alors le graphe Γ_f de f est une relation binaire entre E et F :

$$\Gamma_f = \{(x, f(x)\};$$

2. si E est l'ensemble des points dans le plan $\mathbb{R}^2$ et F est l'ensemble des droites de $\mathbb{R}^2$, alors l'ensemble d'incidence $\mathcal{R} = \{(x, L), x \in E, L \in F \,|\, x \in L\}$ est une relation binaire entre E et F ;
3. si $E = \mathbb{R}$, on a une relation binaire sur E

$$\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R}, \,|\, x \leq y\}.$$

Propriétés des relations binaires :
Soit $\mathcal{R}$ une relation binaire sur l'ensemble E. On dit que la relation $\mathcal{R}$ est

1. *réflexive* si pour tout $x \in E$ on a $x \sim x$;
2. *transitive* si pour tous $x, y, z \in E$ on a
$$x \sim y \text{ et } y \sim z \Rightarrow x \sim z;$$
3. *symétrique* si pour tous $x, y \in E$ on a $x \sim y \Leftrightarrow y \sim x$;
4. *antisymétrique* si pour tous $x, y \in E$ on a
$$x \sim y \text{ et } y \sim x \Leftrightarrow x = y.$$

Définition 1.1.3. Une *relation d'équivalence* sur l'ensemble E est une relation réflexive, transitive et symétrique.

Exemples

1. soit E un ensemble et soit $\mathcal{R}$ la relation $x = y$ (i.e. $\mathcal{R} = \{(x, x)\}$) ;
2. soit $E = \mathbb{N}$, $n \in \mathbb{N}$ un entier fixé et soit $\mathcal{R}$ la relation de congruence $x \equiv y \bmod n$:
$$\mathcal{R} = \{(x, y), n \mid (x - y)\};$$
3. si $f : E \to G$ est une application vers l'ensemble G, la relation
$$\mathcal{R} = \{(x, y) \in E \mid f(x) = f(y)\}$$
est une relation d'équivalence sur E. (En particulier, on obtient le premier exemple pour f l'application identité sur E). On verra dans la suite que toute relation d'équivalence est de cette forme.

Définition 1.1.4. Une *relation d'ordre* sur l'ensemble E est une relation réflexive, transitive et antisymétrique.

Exemples

1. $E = \mathbb{R}$, $\mathcal{R} = \{(x, y) \mid x \leq y\}$;
2. $E = \mathbb{N}$, $\mathcal{R} = \{(x, y) \mid x|y\}$;

Soit $\mathcal{R}$ une relation d'equivalence sur l'ensemble E (par exemple, la relation de congruence modulo 2), on peut alors voir l'ensemble E comme l'union de *classes* des éléments équivalents (par exemple, les nombres paires et impaires) comme suit.

Définition 1.1.5. Soit E un ensemble. Une *partition* de E est un ensemble des parties non vides deux à deux disjointes de E dont E est la réunion.

Exemples

1. $E = \{1, 2, 3, 4, 5, 6\}$ avec une partition $\{1, 2\}, \{3, 5\}, \{4\}, \{6\}$.

2. $E = \mathbb{Z}$ avec une partition $\{n \text{ pair}\}$ et $\{n \text{ impair}\}$.

Définition 1.1.6. Soit E un ensemble. Soit $\mathcal{R}$ une relation d'équivalence sur E. On définit, pour tout $x \in E$

$$\bar{x} = \{y \in E \,|\, x \sim y\}$$

la *classe d'équivalence* de x pour $\mathcal{R}$.

Proposition 1.1.7. *Soit E un ensemble muni d'une relation d'équivalence $\mathcal{R}$. Les différentes classes d'équivalence forment une partition de E.*

Démonstration. Si $x \in E$, alors $x \in \bar{x}$ d'après la réflexivité, donc E est réunion des classes d'équivalences et les classes sont non vides. Il nous reste à montrer que les classes différentes sont disjointes. Supposons le contraire : les classes $\bar{x}$ et $\bar{y}$ sont différentes mais contiennent un élément commun z. Comme $\bar{x}$ et $\bar{y}$ sont différentes, on peut supposer qu'il existe $w \in E$ tel que $w \in \bar{x}$ tel que $w \notin \bar{y}$. On a alors $w \sim x$ et $x \sim z$ donc $w \sim z$ par la propriété de transitivité. Par ailleurs, $z \sim y$, d'où encore $w \sim y$, contradiction. Les classes différentes sont donc disjointes. □

Définition 1.1.8. Soit E un ensemble muni d'une relation d'équivalence $\mathcal{R}$. *L'ensemble quotient* $E/\mathcal{R}$ est l'ensemble des classes d'équivalence pour $\mathcal{R}$. On note $E \to E/\mathcal{R}, x \mapsto \bar{x}$ la surjection (vérifier que c'est une surjection !) canonique.

On voit donc que toute relation d'équivalence provient d'une application : la surjection canonique $E \to E/\mathcal{R}$. Dans l'ensemble $E/\mathcal{R}$ on *identifie* certains éléments de E (ceux qui sont équivalents par la relation $\mathcal{R}$).

Corollaire 1.1.9. *Soit E un ensemble fini muni d'une relation d'équivalence $\mathcal{R}$. Soient $E_1, \dots E_r$ les différentes classes d'équivalence.*

(i) $\mathrm{Card}(E) = \sum_{i=1}^{r} \mathrm{Card}(E_r)$ *;*

(ii) si toutes les classes ont le même nombre d'éléments, on a $\mathrm{Card}(E) = m \cdot \mathrm{Card}(E/\mathcal{R})$.

Exemples

1. $E = \mathbb{Z}$, $\mathcal{R}$ est la relation de congruence modulo n. L'ensemble des classes d'équivalence est noté $\mathbb{Z}/n\mathbb{Z}$.
2. $E = \mathbb{R}$, $\mathcal{R} = \{(x, y) \,|\, x - y \in 2\pi\mathbb{Z}\}$. L'ensemble des classes est noté $\mathbb{R}/2\pi\mathbb{Z}$.

Définition 1.1.10. Soit E un ensemble muni d'une relation d'équivalence $\mathcal{R}$ et soit $f : E \to F$ une application. On dit que f passe au quotient par $\mathcal{R}$ si

$$x \sim y \Rightarrow f(x) = f(y).$$

On peut alors définir une applicaition $\bar{f} : E/\mathcal{R} \to F$ par $\bar{f}(\bar{x}) = f(x)$; cette application est bien définie.

Exemple. $E = \mathbb{R}$, $\mathcal{R} = \{(x, y) \,|\, x - y \in 2\pi\mathbb{Z}\}$. Les applications *sin* et *cos* passent au quotient par $\mathcal{R}$.

Exercices

1. Déterminer si les relations suivantes sont réflexives, transitives, symétriques ou antisymétriques. Dans le cas des relations d'équivalence determiner l'ensemble quotient.
   (a) Soit X un ensemble fini, $E = \mathcal{P}(X)$ est l'ensemble de sous-ensembles de X. Considérer les relations suivantes $\mathcal{R}_1 = \{(X, Y) \,|\, X \subseteq Y\}$, $\mathcal{R}_2 = \{(X, Y) \,|\, X \cap Y = \emptyset\}$.
   (b) $E = \mathbb{Z} \times \mathbb{N}$, $\mathcal{R} = \{((m, n), (m', n')) \,|\, mn' - nm' = 0\}$.
   (c) $E = \mathbb{R}^2 \times \mathbb{R}^2$ est l'ensemble des couples des points du plan réel,

   $$\mathcal{R} = \{((A, B), (A', B')) \,|\, (A = B \text{ et } A' = B') \text{ ou } (AB||A'B' \text{ et } AB = A'B').\}$$

2. Soit E un ensemble non vide. Montrer que toute partition de E peut s'obtenir, de façon unique, à partir d'une relation d'équivalence, comme dans la proposition 1.1.7.
3. Montrer que les applications d'addition et de la multiplication sur $\mathbb{Z}$ passent au quotient par la relation de congruence modulo n.

1.2 Groupes

1.2.1 Définition et premières propriétés

On connait quelques opérations sur l'ensemble des entiers $\mathbb{Z}$: on peut ajouter, multiplier les nombres entiers, on peut alors dire que l'on dispose des applications $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ et $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$. D'une manière générale, on a une définition suivante :

Définition 1.2.1. Soit X un ensemble. Une *loi de composition interne* sur X est une application $X \times X \to X$.

Exemples

1. $X = \mathbb{Z}$ muni de la loi d'addition, de multiplication, de la soustraction ;
2. $X = \mathbb{N}$ muni de la loi d'addition.
3. Soit A un ensemble. Soit X l'ensemble de toutes les applications de A dans A. On a alors que la composition des applications définit une loi de composition interne sur X.

Définition 1.2.2. Une loi de composition interne $*$ sur un ensemble X est dite :
associative si $\forall a, b, c \in X, (a * b) * c = a * (b * c)$,
commutative si $\forall a, b \in X, a * b = b * a$.

Exercice. Lesquelles parmi les lois des exemples précédents sont associatives ? Commutatives ?

Définition 1.2.3. Soit X un ensemble muni d'une loi de composition interne $*$. Un élément $e_g \in X$ est *un élément neutre à gauche* si $\forall a \in X, e_g * a = a$. Un élément $e_d \in X$ est *un élément neutre à droite* si $\forall a \in X, a * e_d = a$.

Exercice. Montrer que s'il existe un élément neutre à gauche et un élément neutre à droite, alors ils coïncident. On appelle l'élément ainsi défini *l'élément neutre* tout court.

Exemple. On a que 0 est l'élément neutre pour l'addition sur $\mathbb{Z}$.

Exercice

1. Trouver un élément neutre à gauche pour la soustraction sur $\mathbb{Z}$. Existe-t-il un élément neutre à droite ?
2. Trouver l'élément neutre pour la multiplication sur $\mathbb{Z}$.

Définition 1.2.4. Un *groupe* est un ensemble G muni d'une loi de composition interne . telle que
(i) . est associative ;
(ii) il existe un élément neutre $e \in G : \forall a \in X, e.a = a.e = a$;
(iii) pour chaque élément $a \in G$ il existe un élément que l'on note $a^{-1} \in G$ et qu'on appelle *l'inverse de* a, tel que $a.a^{-1} = a^{-1}.a = e$.
Si de plus la loi est commutative, on dit que le groupe est *abélien* ou *commutatif*.

Exercice. Soit G un groupe.

1. Soit $a \in G$. Montrer que l'inverse de a est unique.
2. Montrer que pour tout $a \in G$ on a $(a^{-1})^{-1} = a$.
3. Montrer que pour tous $a, b \in G$ on a $(a.b)^{-1} = b^{-1}.a^{-1}$.

Exemples

1. L'ensemble $\mathbb{Z}$ muni de l'addition est un groupe.
2. Le groupe trivial $G = \{0\}$.
3. $G = \mathbb{Z}/n\mathbb{Z}$ muni de l'addition.
4. Le groupe $GL_n(\mathbb{R})$ des matrices inversibles (par multiplication).

5. Soit S_n l'ensemble des bijections de l'ensemble $\{1, \ldots, n\}$ (permutations). Alors l'ensemble S_n muni de la loi de composition est un groupe (non commutatif).
6. Si G et H sont deux groupes, l'ensemble $G \times H$ muni de la loi $(g, h).(g', h') = (g.g', h.h')$ forme un groupe, qu'on appelle le *produit direct* de G et H.

Définition 1.2.5. Soient G et G' deux groupes. Une application $f : G \to G'$ est un *morphisme de groupes* si $f(x.y) = f(x).f(y)$ pour tous $x, y \in G$. Si f est bijective et f^{-1} est aussi un morphisme, on dit que f est un *isomorphisme*, si de plus $G = G'$ on dit que f est un automorphisme.

On dit parfois *homomorphisme* pour un morphisme de groupes.

Exercice. Si $f : G \to G'$ est un morphisme, montrer que $f(e_G) = e_{G'}$, où e_G (resp. $e_{G'}$) est l'élément neutre de G (resp. G'). Montrer que $f(x^{-1}) = f(x)^{-1}$.

Exemples

1. si $G = \mathbb{Z}$, $a \in \mathbb{Z}$, alors $x \mapsto ax$ est un morphisme de G dans lui même.
2. si G est un groupe et $a \in G$ alors la *translation à gauche* $x \to a.x$ n'est pas un morphisme de groupes.
3. si $G = GL_n(\mathbb{R})$, alors le determinant $det : G \to \mathbb{R}$ est un morphisme de groupes.
4. pour tout $g \in G$ l'application $\text{int}_g : G \to G, x \mapsto gxg^{-1}$ est un automorphisme (dit *intérieur*) de G.

1.2.2 Sous-groupes, groupes quotients

Définition 1.2.6. Un sous-ensemble H d'un groupe G est un *sous-groupe* G' s'il vérifie :

- $e \in H$;
- pour tous $x, y \in H$, $xy \in H$;
- pour tout $x \in H$, $x^{-1} \in H$.

On voit donc que l'ensemble H muni de la restriction de la loi du groupe G est lui-même un groupe.

Exemples

1. $H = \{e\}$ est un sous-groupe de G ;
2. les sous-groupes de $\mathbb{Z}$ sont les groupes $n\mathbb{Z}$ des entiers divisibles par n (munis de la loi d'addition).

Proposition 1.2.7. *Soit $f : G \to G'$ un morphisme de groupes, soient H (resp. H') un sous-groupe de G (resp. de G'). Alors*

- *$f(H)$ est un sous-groupe de G', en particulier $Im\, f = f(G)$ est un sous-groupe de G' ;*

- *$f^{-1}(H')$ est un sous-groupe de G, en particulier $Kerf = f^{-1}(e_H)$ est un sous-groupe de G.*

Exemples

1. Le noyau du determinant *det* : $GL_n(\mathbb{R}) \to \mathbb{R}$ est le groupe $SL_n(\mathbb{R})$ des matrices de determinant 1.
2. Pour G un groupe on appelle le *centre* de G le sous-groupe $Z(G)$ (vérifier) formé des éléments qui commutent avec tous les éléments de G :

$$Z(G) = \{x \in G, \mid xg = gx \, \forall g \in G\}.$$

Définition 1.2.8. Soit G un groupe. Un sous-groupe H de G est *distingué* (ou *normal*) s'il est stable par des automorphismes intérieurs : pour tous $g \in G, h \in H$ on a $ghg^{-1} \in H$. On écrit alors $H \triangleleft G$.

Exemples

1. $\{e\}$ et G sont des sous-groupes distingués de G ;
2. si G est abélien, tout sous-groupe de G est dintingué ;
3. $SL_n(\mathbb{R})$ est distingué dans $GL_n(\mathbb{R})$.

Remarque : $\triangleleft$ n'est pas une relation transitive.

Proposition 1.2.9. *Soit $f : G \to G'$ un morphisme de groupes, soient $H \triangleleft G$ et $H' \triangleleft G'$. Alors*

- *$f(H)$ est un sous-groupe distingué dans $f(G)$ (mais pas dans G en général) ;*
- *$f^{-1}(H')$ est distingué dans G, en particulier $Kerf$ est un sous-groupe distingué de G.*

Soient G un groupe et soit $H \subset G$ un sous-groupe de G. On définit une partition de G en classes à gauche (resp. à droite) selon H comme suit :

(**classes à gauche**) $x \sim y$ si $x^{-1}y \in H$: on a $x \sim x$, pour la symétrie on note que si $x^{-1}y \in H$, alors son inverse $y^{-1}x \in H$ et pour la transitivité on remarque que $x^{-1}yy^{-1}z = x^{-1}z$ est donc un élément de H, si $x^{-1}y$ et $y^{-1}z$ le sont. L'ensemble quotient est noté G/H (ses éléments sont les classes aH, $a \in G$).

(**classes à droite**) $x \sim y$ si $xy^{-1} \in H$. On vérifie de même que cela définit une relation d'équivalence. L'ensemble quotient est noté $H \setminus G$ (ses éléments sont les classes Ha, $a \in G$).

Si G est un groupe et $H \subset G$ est un sous-groupe *distingué*, alors on peut munir l'ensemble quotient G/H d'une loi de groupe.

Proposition 1.2.10. *Soit G un groupe et $H \triangleleft G$ est un sous-groupe distingué de G. Alors pour tout $a \in G$ les classes aH et Ha coïncident et $G/H = H \setminus G$. Il*

existe une unique structure de groupe sur G/H telle que la surjection canonique $G \to G/H$ soit un morphisme de groupes.

Démonstration. On a $aH \subset Ha$ car $aHa^{-1} \subset H$ par définition d'un sous-groupe distingué. De même, $Ha \subset aH$ car $a^{-1}Ha \subset H$, d'où les égalités $aH = Ha$ et $G/H = H \setminus G$.

On munit l'ensemble G/H d'une loi $\bar{a}.\bar{b} = \overline{ab}$ (notons que c'est la seule loi que l'on peut considérer si l'on veut que le morphisme $G \to G/H$ soit un morphisme de groupes). Montrons que cette loi est bien définie, i.e ne depend pas de choix de a et b. Soient $a_1 = ah$, $b_1 = bh'$ avec $h, h' \in H$. On a $a_1b_1 = ahbh' = ab(b^{-1}hb)h'$. Comme $b^{-1}hb \in H$ et $h' \in H$, on a bien que la classe de a_1b_1 coïncide avec la classe de ab.

D'après la définition, on voit facilement qu'on définit ainsi une loi de groupe et que la projection $G \to G/H$ est un morphisme de groupes surjectif. □

Exemples. Soit G un groupe et soit $H \triangleleft G$ un sous-groupe distingué de G.

1. L'élément neutre de G/H est la classe $\bar{e} = H$;
2. On peut voir le groupe $\mathbb{Z}/n\mathbb{Z}$ comme quotient du groupe $\mathbb{Z}$ par son sous-groupe $n\mathbb{Z}$.

Remarque. On dit que deux sous-groupes H, H' d'un groupe G sont *conjugués* s'il existe $g \in G$ tel que $H' = gHg^{-1}$.

Proposition 1.2.11. *Soit $f : G \to G'$ un morphisme de groupes. Alors le morphisme f passe au quotient par $H = ker(f)$: il existe un unique homomorphisme $\bar{f} : G/ker(f) \to G'$ tel que $f = \bar{f} \circ \pi$ où π est la surjection canonique $G \to G/ker(f)$. De plus, $\bar{f}$ induit un isomorphisme entre $G/ker(f)$ et $Im(f)$.*

Démonstration. On vérifie que $\bar{f}(\bar{x}) = f(x)$ ne depend pas de choix de l'élement x : si $y \in \bar{x}$, alors $f(x) = f(y)$ par définition de $ker(f)$. Le morphisme $\bar{f}$ est donc bien défini est il est bien un morphisme de groupes. Par ailleurs, $\bar{f}$ est injectif et induit donc un isomorphisme $G/ker(f) \simeq Im(f)$ □

Remarque. Soit $1 \to G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \to 1$ une suite de groupes et de morphismes de groupes. On dit que cette suite est *exacte* si

- f_1 est injectif ($ker(f_1) = e_{G_1}$) ;
- f_2 est surjectif ;
- $Im(f_1) = ker(f_2)$: f_2 induit un isomorphisme $G_2/G_1 \xrightarrow{\sim} G_3$.

Par exemple, la suite

$$1 \to SL_n(\mathbb{R}) \to GL_n(\mathbb{R}) \to \mathbb{R}^* \to 1$$

est une suite exacte.

1.2.3 Groupes finis, groupes cycliques

Définition 1.2.12. Soit G un groupe. Si l'ensemble G est fini, alors le nombre d'éléments de G s'appelle *l'ordre* (ou le *cardinal*) de G.

Exercice. Trouver tous les groupes d'ordre 2, d'ordre 3, dórdre 4.

Théorème 1.2.13 (Théorème de Lagrange)**.** *Soit G un groupe fini. L'ordre de tout sous-groupe H de G divise l'ordre de G.*

Démonstration. Il suffit d'appliquer le corollaire 1.1.9(ii) à la partition de G en classes à gauche selon G : le cardinal de toute telle classe est égal à l'ordre de H. □

Soit G un groupe fini de cardinal n. Soit p un nombre premier qui divise n. Écrivons $n = p^m n'$ où p ne divise pas n'. On peut se demander si G contient un sous-groupe d'ordre p^m. On appelle un tel sous-groupe un *p-Sylow de G*. Le **théorème de Sylow** (que l'on ne démontre ici) affirme que G contient toujours un sous-groupe p-Sylow. Le deuxième théorème de Sylow dit que deux tels sous-groupes sont conjugués.

Proposition 1.2.14. *Soit G un groupe et soit A une partie de G. Il existe un plus petit sous-groupe $H := \langle A \rangle$ contenant A : on l'appelle le sous-groupe engendré par A.*

Démonstration. On définit H comme l'intersection de tous les sous groupes contenant A (vérifier que c'est bien un sous-groupe !). □

Notons que les éléments de A sont de la forme $a = x_1, \dots x_m$ avec soit $x_i \in A$, soit $x_i^{-1} \in A$.

Définition 1.2.15. Soient G un groupe et $g \in G$. *L'ordre* de g est le plus petit entier n, s'il existe, tel que $g^n = 1$. Si $g^n \neq 1$ pour tout $n > 0$ on dit que g est *d'ordre infini.*

Exercice. Montrer que l'ordre de g, s'il est fini, divise l'ordre de G.

Exercice. Soit a un élément de g d'ordre n. Montrer qu'on a alors l'équivalence $a^m = e \Leftrightarrow n \mid m$.

Proposition 1.2.16. *Soient G un groupe et $g \in G$ Si $H = \langle g \rangle$ est infini, alors $H \simeq \mathbb{Z}$. Si H est de cardinal n, alors $H \simeq \mathbb{Z}/n\mathbb{Z}$.*

Démonstration. Dans le premier cas on définit un morphisme $\mathbb{Z} \to \langle g \rangle, m \mapsto g^m$. On voit immédiatement que c'est un morphisme surjectif, il est également injectif car l'ordre de g est infini.

Supposons g est d'ordre n. On a alors un morphisme de groupes bien défini $\mathbb{Z}/n\mathbb{Z}, \bar{m} \mapsto g^m$, dont on vérifie que c'est un isomorphisme. □

Définition 1.2.17. Un groupe G est *monogène* s'il est engendré par un seul élément, *cyclique* s'il est de plus fini.

Exercice. Montrer que si $G = \langle a \rangle$ cyclique d'ordre n, alors

$$G = \langle a^k \rangle \Leftrightarrow (k, n) = 1.$$

Pour les groupes abéliens on dispose du théorème de structure suivant (qui sera démontré dans la deuxième partie : 'Corps finis II'.)

Théorème 1.2.18. *Soit G un groupe abélien engendré par un nombre fini d'éléments. Alors G est isomorphe à*

$$\mathbb{Z}^m \bigoplus_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z},$$

où $m \in \mathbb{N}$ et les entiers n_i vérifient $n_1|n_2|\ldots|n_r$. De plus, m et les n_i sont entièrement déterminés par G.

1.2.4 Groupe symétrique

On note S_n le groupe de permutation de n éléments.

Exercice. Quel est le cardinal de S_n ?

Définition 1.2.19. Une *transposition* $\tau_{i,j}$ est une permutation de la forme suivante : $\tau_{i,j} = \begin{pmatrix} 1 & 2 & \ldots & i & i+1 & \ldots & j & j+1 & \ldots & n \\ 1 & 2 & \ldots & j & i+1 & \ldots & i & j+1 & \ldots & n \end{pmatrix}$

Théorème 1.2.20. *Le groupe S_n est engendré par les transpositions $\tau_{i,j}$, $1 \leq i, j \leq n$.*

Démonstration. Soit f une permutation. Si c'est l'identité, elle est le produit de 0 transpositions. Sinon on considère le premier élément non fixé par f

$$k = \min\{s, 1 \leq s \leq n, f(s) \neq s\}.$$

Alors en appelant τ_1 la transposition qui échange k et $f(k)$, on forme $f_1 = \tau_1 \circ f$. Maintenant le premier élément non fixé par f_1 est plus grand que celui de f. On recommence ensuite avec f_1.

On forme ainsi des permutations f_1, f_2 etc. obtenues en multipliant f par une succession de transpositions τ_1, τ_2 etc. Au bout de l'une des étapes on obtient la permutation identité, car à chaque fois le numéro du premier élément non fixé

par f_i augmente. C'est-à-dire, après l'une des étapes on va obtenir la permutation identique. On a alors

$$(\tau_p \circ \tau_{p-1} \circ \cdots \circ \tau_1) f = \mathrm{Id}.$$

Multiplions cette égalité par $\tau_1 \circ \tau_2 \circ \cdots \circ \tau_p$:

$$\tau_1 \circ \tau_2 \circ \cdots \circ \tau_p \circ \tau_p \circ \tau_{p-1} \circ \cdots \circ \tau_1 \circ f = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_p.$$

Comme $\tau_p \circ \tau_p = \mathrm{Id}$ on peut simplifier la partie gauche :

$$\tau_1 \circ \tau_2 \circ \cdots \circ \tau_{p-1} \circ \tau_{p-1} \circ \cdots \circ \tau_1 \circ f = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_p.$$

De même, on simplifie par $\tau_{p-1} \circ \tau_{p-1} = \mathrm{Id}$ etc. On obtient ainsi $f = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_p$. □

Définition 1.2.21. Soit $s \in S_n$ une permutation. On appelle *signature de* s le produit $\epsilon(s) = \prod_{1 \le i < j \le n} \frac{s(j)-s(i)}{j-i}$. Notons que $e(s) \in \{-1, 1\}$. On appelle *le groupe alterné* A_n le noyau de ϵ. On a donc une suite exacte

$$1 \to A_n \to S_n \to \mathbb{Z}/2\mathbb{Z} \to 1.$$

Soit $x \in \{1, \ldots, n\}$ et soit $\sigma \in S_n$.

Définition 1.2.22. *L'orbite* de x sous l'action de σ est l'ensemble

$$\{x, \sigma(x), \sigma^2(x), \ldots\}.$$

Proposition 1.2.23. *Soit $x \in \{1, \ldots, n\}$ et soit $\sigma \in S_n$. L'orbite de x est finie : il existe k tel que $\sigma^k(x) = x$.*

Démonstration. Résulte du fait que $\{1, \ldots, n\}$ est un ensemble fini. □

Proposition 1.2.24. *Soit $\sigma \in S_n$. Les orbites des éléments de E forment une partition de $\{1, \ldots, n\}$.* □

Définition 1.2.25. Soit $E = \{x_1, x_2, \ldots x_k\} \subset \{1, \ldots, n\}$ un sous-ensemble. On appelle *cycle* $(x_1, x_2, \ldots x_k)$ la permutation σ telle que

- $\sigma(x) = x$ pour $x \notin E$;
- $\sigma(x_j) = x_{j+1}$, $1 \le j < k$;
- $\sigma(x_k) = x_1$.

On appelle l'ensemble E *le support* de σ.

Notons que les cycles $(x_1, x_2, \ldots x_k)$ et $(x_2, \ldots x_k, x_1)$ définissent la même permutation.

Corollaire 1.2.26. *Toute permutation $\sigma \in S_n$ s'écrit comme produit des cycles σ_i à supports disjoints. L'ordre de σ est le p.p.c.m. des ordres des σ_i.*

Démonstration. Réste de la proposition 1.2.24 et de l'observation que chaque orbite définit un cycle. □

1.3 Actions de groupes

> *Un principe directeur des mathématiques modernes tient en cette leçon : lorsque vous avez affaire à une entité S munie d'une certaine structure, essayez de déterminer son groupe d'automorphismes, le groupe des transformations de ses éléments qui préservent les relations structurales. Vous pouvez espérer gagner une profonde compréhension de la constitution de S de cette manière. (Hermann Weyl)*

Définition 1.3.1. Soit G un groupe et soit X un ensemble. Une *action* (à gauche) de G sur X est la donnée d'une application $G \times X \to X, (g, x) \mapsto g.x$ telle que

- pour tout $x \in X$ on a $e.x = x$;
- pour tous $g, g' \in G$ on a $g.(g'.x) = (gg').x$

Exemples

1. $X = G$, *translation à gauche* : $(g, x) \mapsto gx$;
2. $X = G$, *conjugaison* : $(g, x) \mapsto gxg^{-1}$;
3. $G = S_n$ agit sur $E = \{1, \ldots, n\}$ par $s.x = s(x)$.
4. $G = GL_n(\mathbb{R})$ agit sur $\mathbb{R}^n$ par $A.x = Ax$ $(a \in G, x \in X)$.

Définition 1.3.2. Soit X un ensemble muni d'une action d'un groupe G. On appelle

- *orbite* $\omega(x)$ d'un élément $x \in X$ l'ensemble $\{g.x\}$, $g \in G$. S'il n'y a qu'une seule orbite, on dit que G opère *transitivement* sur X [1].
- *stabilisateur* d'un élément $x \in X$ est le sous-groupe H_x

$$H_x = \{g \in G, g.x = x\}.$$

Notons que H_x n'est en général pas distingué. L'action de G est *libre* si tous les stabilisateurs sont réduits à zéro.

Exercice. Determiner les orbites et les stabilisateurs dans les exemples précédents.

Proposition 1.3.3. *Soit X un ensemble muni d'une action d'un groupe G. On a une bijection $G/H_x \to \omega(x), \bar{g} \mapsto g.x$ En particulier, si l'action de G est transitive, elle s'identifie à l'action de G/H_x par les translations à gauche.*

1. cette notion génélarise celle de la section précédente dans le cas de S_n

Démonstration. L'application $\bar{g} \mapsto g.x$ est bien définie : si $\bar{g} = \bar{h}$, alors $h = g.g'$ avec $g' \in H_x$, d'où $h.x = gg'.x = g.x$. On a la surjectivité par la définition de l'orbite. Pour l'injectivité : si $g.x = hx$, alors $h^{-1}g \in H_x$ d'où $\bar{g} = \bar{h}$ dans G/H_x. □

Proposition 1.3.4 (Équation aux classes)**.** *Soit X un ensemble fini muni d'une action d'un groupe fini G. Soit Ω l'ensemble des orbites. Pour tout x soit $\#H_{\omega(x)}$ le cardinal du stabilizateur de l'orbite de x (indépendant du choix de x dans l'orbite d'après la proposition précédente). Alors*

$$\#X = \sum_{\omega \in \Omega} \frac{\#G}{\#H_\omega}.$$

Démonstration. Il suffit de remarquer que les orbites forment une partition de X et appliquer la proposition précédente. □

1.4 Problèmes

1. Soit E un ensemble muni d'une loi de composition, associative, avec élément unité e, et telle que tout élément de E possède un inverse à gauche. Montrer qu'alors tout élément de E possède un inverse à droite qui coïncide avec son inverse à gauche. En déduire que E est un groupe.
2. Soit G un groupe tel que $g^2 = e$ pour tout $g \in G$. Montrer que G est abélien.
3. Soient G et H des groupes cycliques à m et n éléments. Montrer que, pour que $G \times H$ soit cyclique il faut et il suffit que m et n soient premiers entre eux.
4. Soit A une partie d'un groupe G.
   (a) On appelle *centralisateur* de A dans G l'ensemble $Z(A)$ des $x \in G$ tels que $xa = ax$ pour tout $a \in A$. Montrer que $Z(A)$ est un sous-groupe de G. Montrer que $Z(G)$ (le centre de G) est un sous-groupe commutatif et distingué de G.
   (b) On note sAs^{-1} (pour $s \in G$ donné) l'ensemble des éléments de G de la forme sxs^{-1} avec $x \in A$. Montrer que si A est un sous-groupe, il en est de même de sAs^{-1}. On appelle *normalisateur* d'un sous groupe A de G l'ensemble $N(A)$ des $s \in G$ tels que $sAs^{-1} = A$. Montrer que le centralisateur de A est un sous-groupe distingué du normalisateur de A.
5. (**Groupe diédral**)
   (a) On considère l'ensemble D_{2n} des isométries qui préservent un polygone régulier à n cotés (n est un entier ≥ 3). Montrer que c'est un groupe, le groupe diédral, que ce groupe a $2n$ éléments, dont la moitié sont des rotations (d'angle multiple de $2\pi/n$) et les autres des réflexions (d'ordre 2). Ce groupe est-il commutatif ?

(b) Montrer que D_{2n} est isomorphe à un sous-groupe de S_n.

(c) Montrer que le sous-groupe des rotations est distingué (par exemple en l'exhibant comme noyau d'un morphisme de groupes), mais que le sous-groupe engendré par une réflexion ne l'est pas.

6. (**Groupes de matrices**)

(a) Déterminer le centre de $GL_n(\mathbb{R})$.

(b) Montrer que

$$O(n) = \{g \in GL_n(\mathbb{R}) \,|\, {}^t g^{-1} = g\}$$

est un sous-groupe de $GL_n(\mathbb{R})$. Vérifier que c'est le groupe des isométries vectorielles de l'espace $\mathbb{R}^n$. Déterminer tous les éléments de $O(2)$.

(c) Montrer que

$$O^+(n) = \{g \in O(n), det(g) = 1\}$$

est un sous-groupe distingué de $O(n)$. Déterminer tous les éléments de $O^+(2)$ et montrer que c'est un groupe commutatif. En est-il de même de $O(2)$? De $O^+(n)$ avec $n \geq 3$?

(d) Soit $\mathbb{H}_8$ le sous-groupe de $GL_2(\mathbb{C})$ engendré par les matrices

$$I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},\ K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.$$

Calculer l'ordre de $\mathbb{H}_8$. Exhibez tous ses sous-groupes, ses sous-groupes distingués, son centre, et ses quotients. En déduire que tous les sous-groupes propres sont distingués et cycliques.

7. (**Formule de Burnside**) Soit G un groupe fini opérant sur un ensemble fini X. Pour tout $g \in G$, notons $\mathrm{Fix}(g)$ le sous-ensemble de X constitué des points fixes de g. Soit E l'ensemble des couples (g, x) de $G \times X$ qui vérifient $g.x = x$.

(a) Montrer que le cardinal de E est $\sum_{g \in G} \#\mathrm{Fix}(g)$.

(b) Par ailleurs, montrer que le cardinal de E est $\sum_{x \in X} \frac{\#G}{\#\omega(x)}$.

(c) En déduire la formule $\sum_{x \in X} \frac{1}{\#\omega(x)} = \frac{1}{\#G} \sum_{g \in G} \#\mathrm{Fix}(g)$. Montrer que ce nombre est égal au nombre d'orbites.

(d) En déduire que si $P_n(k)$ est le nombre de permutations de $\{1, \ldots, n\}$ qui ont exactement k points fixes, alors $\sum_{k=0}^{n} k P_n(k) = n!$

8. Soit G un groupe fini, d'ordre une puissance d'un nombre premier p.

(a) Supposons que G agit sur un ensemble fini X dont le cardinal n'est pas une puissance de p. Montrer que G admet au moins un point fixe dans X.

(b) En faisant opérer G sur lui même par des automorphismes intérieurs, montrer que le centre de G n'est pas réduit à l'élément neutre.

(c) Soit G un groupe. Montrer que si $G/Z(G)$ est un groupe cyclique, alors G est abélien.

(d) Soit p est un nombre premier. Montrer qu'un groupe de cardinal p^2 est commutatif. (Montrer qu'un tel groupe est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$).

9. (**Théorème de Sylow**) Soit G un groupe tel que $|G| = n = p^r m$ avec $(p, m) = 1$. On considère l'ensemble X des parties de G de cardinal p^r et l'ensemble Y des p-sous-groupes de Sylow de G.

   (a) On fait opérer G sur X par translations à gauche. Soit $E \in X$, G_E le stabilisateur de E. Montrer qu'on a $|G_E| \leq p^r$.

   (b) Montrer que $|G_E| = p^r$ si et seulement si $E = Sx$ avec $x \in G$ et $S \in Y$. Montrer qu'alors on a $S = G_E$.

   (c) En déduire, en considérant les orbites X sous G, la congruence $|X| \equiv m|Y| \pmod{p}$.

   (d) Montrer qu'on a $|X| \equiv m \pmod{p}$ (soit par un calcul direct, soit en appliquant c) à $\mathbb{Z}/n\mathbb{Z}$).

   (e) Démontrer la congruence $|Y| \equiv 1 \pmod{p}$.

Chapitre 2

Anneaux

2.1 Anneaux, idéaux, anneaux quotient

Un exemple d'un groupe abélien est l'ensemble $\mathbb{Z}$ muni de l'addition. De plus, sur cet ensemble on définit habituellement la loi de multiplication. C'est-à-dire, l'ensemble $\mathbb{Z}$ est muni naturellement de deux lois de composition interne. Cet exemple nous amène à la définition d'un anneau.

Définition 2.1.1. Un *anneau* est un ensemble A muni de deux lois de composition interne $+, *$ telles que

(i) $(A, +)$ est un groupe abélien ;

(ii) la loi $*$ est associative, munie d'un élément neutre [1] ;

(iii) la loi $*$ est distributive par rapport à la loi $+$, c'est-à-dire,

$$a * (b + c) = a * b + a * c \text{ et}$$
$$(b + c) * a = b * a + c * a$$

pour tous $a, b, c \in A$.

Si la loi $*$ est commutative, on dit que A est un anneau *commutatif*. Dans la suite on se limitera à l'étude des anneaux commutatifs (et on dira donc «anneau» pour «anneau commutatif»).

Remarque. Si A est un anneau, on note souvent 0 l'élément neutre de la loi $+$ et 1 l'élément neutre de la loi $*$, de même comme dans le cas $A = \mathbb{Z}$.

Exemples

1. $(\mathbb{Z}, +, \times)$ est un anneau qu'on appelle *l'anneau des entiers relatifs.*
2. l'anneau nul $\{0\}$;
3. $(\mathbb{Z}/n\mathbb{Z}, +, \times)$;

1. On utilise aussi la terminologie 'anneau unitaire' dans le cas où la loi $*$ est munie d'un élément neutre.

4. si A est un anneau (commutatif), on a aussi l'anneau des polynômes $A[x_1, x_2, \ldots, x_n]$ à coefficients dans A ;
5. de même comme dans le cas des groupes, si A et A' sont deux anneaux, on définit la structure d'anneau sur le produit direct $A \times A'$.
6. l'ensemble des fonctions continues $f : \mathbb{R} \to \mathbb{R}$ avec l'addition et la multiplication usuelle est un anneau.

Définition 2.1.2. Un *corps* est un anneau non nul dans lequel tout élément non nul admet un inverse pour la loi de multiplication $\times$.

Exemples : $\mathbb{Q}, \mathbb{C}, \mathbb{R}, \mathbb{Z}/p\mathbb{Z}$ où p est un nombre premier (voir le chapitre suivant pour ce dernier).

De façon générale, l'ensemble des éléments inversibles d'un anneau A forme un groupe pour la multiplication que l'on note A^* :

$$A^* = \{a \in A, \exists b \in A \,|\, ab = 1\}.$$

Définition 2.1.3. Soit A un anneau. On dit que A est *intègre* si la condition $ab = 0$ avec $a, b \in A$ implique que $a = 0$ ou $b = 0$.

Exemples.

1. $\mathbb{Z}$ est un anneau intègre ;
2. $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier ;
3. si A est intègre, alors $A[x_1, \ldots x_n]$ est intègre.

Si A est un anneau intègre, on appelle *corps des fractions* $\operatorname{Frac} A$ de A le plus petit corps contenant A. Par exemple, $\operatorname{Frac} \mathbb{Z} = \mathbb{Q}$, $\operatorname{Frac} \mathbb{R}[x] = \mathbb{R}(x)$ est le corps des fractions rationnelles à une variable sur $\mathbb{R}$.

Définition 2.1.4. Un *morphisme* (ou un *homomorphisme* d'anneaux) est une application $f : A \to B$ telle que

- $f(1) = 1$;
- $f(x + y) = f(x) + f(y)$;
- $f(xy) = f(x)f(y)$;

Définition 2.1.5. Une partie $B \subset A$ d'un anneau A est un sous-anneau si la restriction de la structure d'anneau sur A définit une structure d'anneau sur B, autrement dit, si

- $1 \in B$;
- $(B, +)$ est un sous-groupe de $(A, +)$;
- B est stable par la multiplication interne.

Exemple : $\mathbb{Z}$ est un sous-anneau de $\mathbb{Z}[x]$.

Exercice. Soit $A[x_1, \dots x_n]$ l'anneau des polynômes à coefficients dans A. Montrer qu'on a la *propriété universelle* suivante : si B est un anneau, alors la donnée d'un morphisme $A[x_1, \dots x_n] \to B$ est équivalente à la donnée de n éléments $b_1, \dots, b_n$ de B.

Définition 2.1.6. Une partie $I \subset A$ est un **idéal** de A si I est un sous-groupe de A pour l'addition et si, pour tout $x \in I$ et tout $a \in A$, on a $ax \in I$.

Exemples :

1. $I = \{0\}, I = A$;
2. pour $n \in \mathbb{Z}$ on définit $n\mathbb{Z} = \{x \in \mathbb{Z}, n \,|\, x\}$, qui est un idéal de $\mathbb{Z}$.
3. Si $S \subset A$ est une partie finie de A, on définit **l'idéal de A engendré par** S comme l'ensemble des sommes finies :
$$(S) = \{x = \sum_i s_i a_i, s_i \in S, a_i \in A\}.$$
4. Si $f : A \to B$ est un morphisme d'anneaux, alors $ker(f)$ est un idéal de A.

Exercice. Soient $I, J \subset A$ des idéaux dans A. Montrer que les ensembles suivants sont des idéaux dans A :

1. $I + J = \{x + y, x \in I, y \in J\}$
2. $I \cdot J$ l'idéal engendré par $\{xy, x \in I, y \in J\}$;
3. $I \cap J = \{x \in A \,|\, x \in I \text{ et } x \in J\}$.

Si $I \subset A$ est un idéal, on peut munir le groupe quotient A/I de la loi multiplicative :
$$\bar{a} \cdot \bar{b} = \overline{ab}.$$
On vérifie que cette opération est bien définie, i.e. ne dépend pas de choix de représentants a et b : si $a_1 = a + i$, $b_1 = b + j$ avec $i, j \in I$, on a $a_1 b_1 = ab + ib + ja + ij$ avec $ib + ja + ij \in I$ et on a donc bien l'égalité de classes.

On voit donc que l'ensemble A/I forme un anneau, appelé *l'anneau quotient* A/I.

Exemples :

1. l'anneau $\mathbb{Z}/n\mathbb{Z}$ est le quotient de l'anneau $\mathbb{Z}$ par l'idéal (n) engendré par n ;
2. $\mathbb{R}[x]/(x) \simeq \mathbb{R}$;
3. $\mathbb{R}[x, y]/(x) \simeq \mathbb{R}[y]$;
4. la classe $\bar{x}$ dans $\mathbb{R}[x]/(x^2)$ vérifie $\bar{x}^2 = 0$;

5. $\mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$.

Proposition 2.1.7. *Soit $f : A \to B$ un morphisme d'anneaux. Alors il existe un unique morphisme d'anneaux $\bar{f} : A/ker(f) \to B$ tel que $f = \bar{f} \circ \pi$ où π est la surjection canonique $A \to A/ker(f)$. De plus, $\bar{f}$ induit un isomorphisme d'anneaux entre $A/ker(f)$ et $Im(f)$.*

Démonstration. Laissée en exercice. □

Définition 2.1.8. Un idéal I est **premier** si A/I est un anneau intègre. Un idéal I est **maximal** si A/I est un corps.

Proposition 2.1.9. *Un idéal I est maximal si $I \neq A$ et si pour tout idéal J contenant I on a soit $I = J$ soit $J = A$.*

Démonstration. Supposons que A/I est un corps. Soit J un idéal $I \subset J$ avec $J \neq I$. Soit $x \in J \setminus I$, on a donc que $\bar{x}$ est inversible dans A/I : $\exists \bar{y} \in A/I$ la classe de y telle que $\bar{x}.\bar{y} = \bar{1}$, i.e. $1 = xy + i$ avec $i \in I$ et $xy \in J$, donc $1 \in J$ et $J = A$.

Supposons maintenant que pour tout idéal J contenant I on a soit $I = J$ soit $J = A$. Montrons que A/I est un corps. Soit $\bar{x} \in A/I$ une classe non nulle. L'idéal J engendré par x et I contient strictement I, on a donc $J = A$. En particulier, $1 \in J$, i.e. $\exists y \in A$ et $i \in I$ tels que $1 = xy + i$, d'où $\bar{x}.\bar{y} = \bar{1}$. □

Exemples :

1. L'idéal $n\mathbb{Z}$ de $\mathbb{Z}$ est premier si et seulement si n est premier. L'idéal $\{0\}$ est aussi premier dans $\mathbb{Z}$.
2. L'idéal (x) est maximal dans l'anneau $k[x]$ des polynômes à coefficients dans un corps k. Plus généralement, pour tout $a \in k$, l'idéal $(x - a)$ est maximal.

On a un énoncé suivant, dont la preuve découle du lemme de Zorn (et utilise donc l'axiome de choix) :

Théorème 2.1.10 (Krull). *Tout idéal $I \neq A$ d'un anneau A est inclus dans un idéal maximal.*

2.2 Divisibilité dans les anneaux

2.2.1 Anneaux principaux

Soit A un anneau (commutatif) intègre. On a une notion de divisibilité des éléments de A, analogue à celle de divisibilité de nombres entiers.

Définition 2.2.1. Soient $a, b \in A$. On dit que a divise b s'il existe $c \in A$ tel que $b = ac$. On écrit alors $a \mid b$.

Notons que $a \mid b \Leftrightarrow (b) \subset (a)$.

Proposition 2.2.2. *On a* $(a \mid b)$ *et* $(b \mid a) \Leftrightarrow a = ub, u \in A^*$.

Démonstration. laissée en exercice.

Dans la situation de la proposition précédente on dit que a et b sont *associés*.

Définition 2.2.3. On dit que $p \in A$ est *irréductible* si p n'est pas inversible et si

$$p = ab \Rightarrow a \text{ ou } b \text{ est inversible.}$$

On dit que $a, b \in A$ sont premiers entre eux s'ils n'ont pas de diviseurs communs autres que les éléments de A^*.

Exemples :

1. si p est un nombre premier, alors p est irrédictible dans $\mathbb{Z}$;
2. l'élément $x^2 + 1$ est irréductible dans $\mathbb{R}[x]$.

Définition 2.2.4. Un anneau A est **principal** s'il est intègre et si tous ses idéaux sont de la forme $(x) = x\,A$ avec $x \in A$.

Exemples :

1. $\mathbb{Z}$;
2. $k[x]$ où k est un corps.

Pour A un anneau principal on a un analogue du théorème de Bézout :

Théorème 2.2.5. *Soit A un anneau principal. Soient $a, b \in A$. Alors a et b sont premiers entre eux si et seulement si $(a, b) = A$, i.e. s'il existent $u, v \in A$ tels que $ua + vb = 1$.*

Démonstration. Supposons que a et b sont premiers entre eux. Puisque A est un anneau principal, il existe $d \in A$ tel que $(a, b) = (d)$, en particulier d est un diviseur commun de a et b, d'où $d \in A^*$ et $(a, b) = 1$.

Inversement, s'ils existent $u, v \in A$ tels que $ua + vb = 1$, alors tout diviseur commun de a et b divise aussi 1 et il est donc inversible. □

2.2.2 Algorithme d'Euclide étendu

L'anneau des entiers $\mathbb{Z}$ est un anneau principal. En particulier, comme dans la preuve du théorème de Bézout, pour deux entiers a et b le plus grand diviseur commun d de a et b est le générateur de l'idéal (a, b), i.e. $(a, b) = (d)$ et ils existent $u, v \in \mathbb{Z}$ tels que $au + bv = d$. On rappelle l'algorithme d'Euclide qui permet de trouver a et b et l'on décrit l'algorithme d'Euclide étendu qui permet de trouver u et v.

Algorithme d'Euclide
Données : $a, b \in \mathbb{Z}$.
Sortie $d = pgcd(a, b)$

1. $a_1 := a$, $b_1 = b$;
2. tant que $b_1 \neq 0$
   - calculer le reste r de la division de a_1 par b_1 : $a_1 = b_1 q + r, 0 \leq r < b_1$
   - $a_1 := b_1$, $b_1 := r$;
3. retourner a_1.

Algorithme d'Euclide étendu
Données : $a, b \in \mathbb{Z}$.
Sortie $d = pgcd(a, b)$ et $u, v \in \mathbb{Z}$ avec $d = au + bv$.

1. $a_1 := a$, $b_1 = b$;
2. $s_0 = 1$; $t_0 = 0$, $s_1 = 0$, $t_1 = 1$. *Notons qu'on a* $a_1 = as_0 + bt_0$ *et* $b_1 = as_1 + bt_1$.
3. tant que $b_1 \neq 0$
   - calculer le reste r de la division de a_1 par b_1 : $a_1 = b_1 q + r, 0 \leq r < b_1$
   - $a_1 := b_1$;
   - $b_1 := r$;
   - $x := s_0 - qs_1$, $y = t_0 - qt_1$;
   - $s_0 := s_1$, $t_0 := t_1$, $s_1 := x$; $t_1 := y$. *Notons que on a encore* $a_1 = as_0 + bt_0$ *et* $b_1 = as_1 + bt_1$.
4. retourner $d = a_1, u = s_0, v = t_0$. Comme on a après chaque étape $a_1 = as_0 + bt_0$ par construction, on obtient bien $d = au + bv$.

2.2.3 Anneaux factoriels

Définition 2.2.6. Un anneau intègre A est dit **factoriel** si tout élément non nul $a \in A$ peut s'écrire de façon unique, à une permutation de facteurs et à une multiplication par des inversibles près, comme

$$(*)\, a = up_1 \dots p_n,$$

où $u \in A$ est inversible et $p_1, \dots p_n$ sont des éléments irréductibles.

Exemples et propriétés :

1. $\mathbb{Z}$ est factoriel ;
2. $k[x]$ est factoriel ;
3. plus généralement, un anneau principal est factoriel (c'est un théorème non trivial : voir plus loin) ;
4. le théorème de Gauss (que l'on ne démontre pas ici) dit que si A est un anneau factoriel, alors l'anneau $A[x]$ est aussi factoriel ; en particulier, $k[x_1, \ldots, x_n]$ est factoriel. Notons que pour $n \geq 2$ cet anneau n'est pas principal.
5. l'anneau $\mathbb{Z}[\sqrt{-5}] = \mathbb{Z}[T]/(T^2+5)$ n'est pas factoriel : on a $9 = 3 \times 3 = (2-\sqrt{-5})(2+\sqrt{-5})$ et on montre que 3, $2-\sqrt{-5}$ et $2+\sqrt{-5}$ sont irréductibles, mais que 3 n'est pas associé à $2-\sqrt{-5}$, ni à $2+\sqrt{-5}$. Cela montre aussi qu'un quotient d'un anneau factoriel n'est pas nécessairement factoriel.
6. Si A est factoriel, on choisit un ensemble $\mathcal{P}$ des éléments irréductibles non-associés. En particulier, si $p, q \in A$, alors p et q sont premiers entre eux. On peut alors écrire (en regroupant les premiers dans (*) qui coïncident) pour tout $a \in A$, $a = u p_1^{v_{p_1}(a)} \ldots p_n^{v_{p_n}(a)}$ avec $p_i \in \mathcal{P}$ et $v_{p_i}(a)$ des entiers positifs. On pose $v_p(a) = 0$ si $p \in \mathcal{P}$ est distinct des $p_1, \ldots p_n$.

Proposition 2.2.7. *Soit A un anneau intègre tel que tout élément non nul de A s'écrit comme produit des éléments irrédictibles. Les propriétés suivantes sont équivalentes :*

(i) A est factoriel ;

(ii) [lemme de Gauss] : si $a, b, c \in A$, alors on a

$$a \,|\, bc, (b, a) = 1 \Rightarrow a \,|\, c;$$

(iii) si $p \in A$ est irréductible, alors l'idéal (p) est premier.

Démonstration. $(i) \Rightarrow (ii)$. On choisit un ensemble $\mathcal{P}$ des éléments irréductibles non-associés de A. Puisque $a \,|\, bc$, on a $v_p(a) \leq v_p(b) + v_p(c)$. Comme $(b, a) = 1$, on a $v_p(a) > 0 \Rightarrow v_p(b) = 0$ et donc $v_p(a) \leq v_p(c)$ pour tout p (pour p tel que $v_p(a) = 0$ cette assertion est évidente.) Ainsi $a \,|\, c$.

$(ii) \Rightarrow (iii)$ Il s'agit de montrer que si p est irréductible et $p \,|\, ab$ alors $p \,|a$ ou $p \,|\, b$, ce qui est un cas particulier de (ii).

$(iii) \Rightarrow (i)$ Il s'agit de montrer que la décomposition (*) est unique à une permutation de facteurs et à une multiplication par des inversibles près. Sinon on a une égalité $u \prod_{p \in \mathcal{P}} p^{n_p} = v \prod_{p \in \mathcal{P}} p^{m_p}$ avec $n_p \neq m_p$ pour au moins un irréductible p. On a donc que p divise le produit $p_1^{n_1} \ldots p_r^{n_r}$ avec $p_i \neq p \, \forall i$. D'après (iii) p divise donc un des $p_i^{n_i}$, contradiction.

□

On voit en particulier que les notions de *plus grand diviseur commun pgcd*, ainsi que de *plus petit multiple commun ppcm* sont bien définies dans les anneaux factoriels, à une multiplication par un élément inversible près.

Pour pouvoir appliquer le théorème précédent, on aura donc besoin de déterminer si dans un anneau A on peut décomposer tout élément en produit des éléments irréductibles.

Définition 2.2.8. Un anneau A est dit *noethérien* si tout idéal de A peut être engendré par un nombre fini d'éléments.

Exercice. Montrer que A est noethérien si et seulement si toute suite croissante $I_1 \subseteq I_2 \subseteq \dots I_n \subseteq \dots$ d'idéaux de A est stationnaire : $\exists n_0 \,|\, \forall n \geq n_0 \; I_n = I_{n_0}$.

Exemples et propriétés :

1. un anneau principal est noethérien ;
2. le théorème de Hilbert (que l'on ne démontre pas ici) dit que si A est un anneau noethérien, alors l'anneau $A[x]$ est aussi noethérien ; en particulier, $A[x_1, \dots, x_n]$ est alors aussi noethérien.

Proposition 2.2.9. *Soit A un anneau noethérien intègre. Alors tout élément non nul de A s'écrit comme produit*
$(*)\, a = up_1 \dots, p_n$, *où $u \in A$ est inversible et $p_1, \dots p_n$ sont des éléments irréductibles.*

Démonstration. Supposons le contraire. Soit aA l'idéal de A maximal pour l'inclusion dans l'ensemble des idéaux xA avec x n'admettant pas la décomposition (*) (un tel a existe car A est noethérien). En particulier a n'est pas irréductible et on peut donc écrire $a = bc$. D'après le choix de a, les éléments b et c admettent une décomposition (*), donc a aussi, contradiction. □

Corollaire 2.2.10. *Un anneau principal est factoriel.*

Démonstration. Si A est un anneau principal, il est en particulier noethérien et donc tout élément s'écrit comme produit des éléments irréductibles. Par ailleurs, si $p \in A$ est irréductible, alors (p) est maximal (en particulier, premier) car si $(p) \subset (x)$ on a $p = xy$ et alors soit $x = p$ soit x est inversible. On peut donc appliquer la proposition 2.2.7. □

Une autre propriété d'anneaux généralise la notion de la division euclidienne :

Définition 2.2.11. Un anneau *euclidien* est un anneau A muni d'une application $v : A \setminus \{0\} \to \mathbb{N}$ telle que pour tous $a, b \in A$ non nuls il existent $q, r \in A$ (non nécessairement uniques) tels que

- $a = bq + r$;
- $r = 0$ ou $v(r) < v(b)$.

Exemples

1. $\mathbb{Z}$, $v(x) = |x|$;
2. $k[x]$ où k est un corps, $v(P) = deg(P)$.

Remarque. L'algorithme d'Euclide s'étend à un anneau euclidien.

Proposition 2.2.12. *Un anneau euclidien est principal.*

Démonstration. Soit $I \subset A$ un idéal non nul et soit $b \in I$ non nul avec $v(b)$ minimal dans I. Puisque A est euclidien, tout $a \in I$ s'écrit $a = bq + r$ avec $r = 0$ ou $v(r) < v(b)$. Par le choix de b on a nécessairement $r = 0$ et donc $I = (b)$. □

Remarque Il existe des anneaux principaux non euclidiens (par exemple, on peut montrer que l'anneau $\mathbb{R}[x, y]/(x^2 + y^2 + 1)$ est un anneau principal non euclidien.)

2.3 Problèmes

1. Soit A un anneau. Un élément $a \in A$ est nilpotent s'il existe $n \in \mathbb{N}$ tel que $a^n = 0$.
   (a) Montrer que l'ensemble $Nil(A)$ des éléments nilpotents de A est un idéal.
   (b) Montrer que si I est un idéal premier de A, on a $Nil(A) \subset I$.
2. (a) Calculer le pgcd de $P = 2X^4 - 3X^2 + 1$ et $Q = X^3 + X^2 - X - 1$ dans $\mathbb{Q}[X]$ et $U, V \in \mathbb{Q}[X]$ tels que $pgcd(P, Q) = UP + VQ$. Même question dans $\mathbb{R}[X]$.
   (b) Calculer l'inverse de $X^3 - X + 1$ dans $\mathbb{Q}[X]/(X^2 + X + 1)$.
   (c) Calculer $pgcd(X^n - 1, X^m - 1)$.
3. (a) Donner un exemple d'anneau factoriel non principal.
   (b) Soit $A = \mathbb{C}[X, Y]/(X^3 - Y^2 - X)$. Montrer que A n'est pas factoriel (si x, y sont des images dans A des X, Y par la projection canonique $\mathbb{C}[X, Y] \to A$, montrer que y est irréductible mais que l'idéal (y) n'est pas premier.)
4. (**L'anneau des entiers de Gauss**) On considère l'anneau des entiers de Gauss
$$\mathbb{Z}[i] = \{a + bi, a, b \in \mathbb{Z}\}.$$
On pose $N(a + bi) = a^2 + b^2$.
   (a) Montrer que $N(xy) = N(x)N(y)$. En déduire les éléments inversibles de $\mathbb{Z}[i]$.
   (b) Si $x \in \mathbb{Z}[i]$ et si $N(x)$ est un entier premier, montrer que x est irréductible. La réciproque est-elle vraie ?
   (c) Soient $x, y \in \mathbb{Z}[i]$ avec y non nul. On pose $\frac{x}{y} = u + iv$ où $(u, v) \in \mathbb{Q}^2$. Soit $(u_0, v_0) \in \mathbb{Z}^2$ tel que $|u - u_0| \leq \frac{1}{2}$ et $|v - v_0| \leq \frac{1}{2}$. Montrer qu'on a $x = y(u_0 + iv_0) + r$ avec $N(r) < N(y)$. Dans quel cas $u_0 + iv_0$ et r sont uniques ?

(d) En déduire que $\mathbb{Z}[i]$ est principal.

(e) Soit p un nombre premier dans $\mathbb{Z}$. Montrer que p est irréductible dans $\mathbb{Z}[i]$ si et seulement s'il n'existe pas $(a, b) \in \mathbb{N}^2$ tel que $p = a^2 + b^2$.

(f) Montrer que si p est un nombre premier tel que $p \equiv 3 \pmod 4$, alors

$$a^2 + b^2 \equiv 0 \pmod p \Rightarrow a \equiv 0 \pmod p \text{ et } b \equiv 0 \pmod p.$$

En déduire que tout nombre premier ≥ 3 est irréductible dans $\mathbb{Z}[i]$ si et seulement si $p \equiv 3 \pmod 4$.

(g) Montrer qu'un entier n est une somme de deux carrés si et seulement si pour tout premier $p \equiv 3 \pmod 4$ divisant n, on a $n = p^{2r}m$ avec $(m, p) = 1$.

(h) Montrer que $x = a+bi \in \mathbb{Z}[i]$ est irréductible si et seulement si on a l'une de deux conditions suivantes :

i. $N(x)$ est un nombre premier ;

ii. $N(x)$ est un carré d'un nombre premier de la forme $4k + 3$.

5. (**Un exemple d'anneau principal non euclidien**) On considère le sous-anneau A de $\mathbb{C}$ engendré par $\alpha = (1 + i\sqrt{19})/2$:

$$A = \mathbb{Z}[\alpha].$$

(a) Vérifier que $\alpha^2 - \alpha + 5 = 0$. Montrer que $A = \{a + b\alpha, a, b \in \mathbb{Z}\}$.

(b) Montrer que A est stable par conjugaison. On définit $N(z) = z\bar{z}$ pour $z \in A$. À l'aide de N, décrire A^*.

(c) Soit R un anneau euclidien, alors il existe $x \in R \setminus R^*$ tel que la restriction de la surjection naturelle $\pi : R \to R/(x)$ à $R^* \cup \{0\}$ est surjective. Montrer que $R/(x)$ est un corps.

(d) Montrer que A n'est pas euclidien.

(e) Soient $z, z' \in A$ non nuls. Montrer qu'ils existent $q, r \in A$ vérifiant les deux conditions suivantes :

i. N(r)<N(z') ;

ii. $z = z'q + r$ ou $2z = z'q + r$.

(Indication : écrire $z/z' = u+v\alpha$ avec $u, v \in \mathbb{Q}$, pour $n = E(v)$ considérer les cas $v \in]n + \frac{1}{3}, n + \frac{2}{3}[$ ou pas.)

(f) Montrer que (2) est un idéal maximal de A (Indication : vérifier que A est isomorphe à l'anneau $\mathbb{Z}[X]/X^2 - X + 5$).

(g) Montrer que A est principal.

Chapitre 3

Corps

3.1 Extensions de corps

Rappelons qu'un corps est un anneau commutatif dans lequel tout élément non nul est inversible.

Exemples

1. $\mathbb{R}, \mathbb{C}, \mathbb{R}(x)$;
2. un *corps premier*, qui est par définition soit le corps des nombres rationnels $\mathbb{Q}$, soit le corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ où p est un nombre premier.

Définition 3.1.1. Soit K un corps. Une *extension* de K est un corps L tel que K est un sous-corps de L (i.e. $K \subset L$).

Par exemple, si on a $f : K \to L$ un morphisme injectif de corps, on peut voir K comme un sous-corps de L en identifiant $f(K) \simeq K$.

Si L est une extension de K, on dispose d'une structure de K-espace vectoriel sur L via multiplication.

Définition 3.1.2. Si L est de dimension finie sur K, on dit que L est une extension *finie* de K, on note $[L : K]$ la dimension du K-espace vectoriel L et on l'apelle le *degré* de L sur K.

Proposition 3.1.3. *Soit $K \subset L \subset F$ des extensions des corps. Si $e_i, i \in I$ est une base de L sur K et si $\epsilon_j, j \in J$ est une base de F sur L, alors $(e_i\epsilon_j)_{(i,j)\in I\times J}$ est une base de F sur L.*

Démonstration. Supposons

$$\sum_{(i,j)\in I\times J} \lambda_{ij} e_i \epsilon_j = 0$$

ou tous les coefficients $\lambda_{ij} \in K$ sauf un nombre fini sont nuls. On a alors

$$\sum_{j\in J} \epsilon_j \sum_{i\in I} \lambda_{ij} e_i = 0,$$

d'où $\sum_{i\in I} \lambda_{ij} e_i = 0$ (la famille ϵ_j est libre), d'où $\lambda_{ij} = 0$ pour tous i, j (e_i est une famille libre). On a donc que $(e_i\epsilon_j)_{(i,j)\in I\times J}$ est une famille libre.

Si maintenant $x \in F$, on peut écrire $x = \sum_{j\in J} a_j\epsilon_j$ où $a_j \in L$. On peut donc écrire $a_j = \sum a_{ij}e_j$, $a_{ij} \in K$ on voit donc que x est une combinaison linéaire des $e_i\epsilon_j$ avec coefficients dans K. □

Corollaire 3.1.4. *Si $K \subset L \subset F$ sont des extensions finies, on a*

$$[F : K] = [F : L] \cdot [L : K].$$

Définition 3.1.5. Soit L/K une extension et soit $\alpha \in L$. On note $K[\alpha]$ le sous-anneau de L engendré par K et α (i.e. $K[\alpha]$ est l'ensemble des polynômes $P(\alpha)$ avec $P \in K[T]$. On note $K(\alpha)$ le sous-corps de L engendré par K et α (i.e. $K(\alpha)$ est le corps des fractions de $K[\alpha]$ et est l'ensemble des $R(\alpha)$ avec $R \in K(T)$).

Soient L/K une extension de corps et $\alpha \in L$. On définit un morphisme d'anneaux $f : K[T] \to L$ par $P \mapsto P(\alpha)$.

Définition 3.1.6. Si f est injectif, on dit que α est *transcendant* sur K : on a $K[\alpha] \simeq K[T]$ et $K(\alpha) \simeq K(T)$. Si f n'est pas injectif, on dit que α est algébrique sur K, si P est le générateur de $ker(f)$ on appelle P le polymôme minimal de α sur K.

Remarque. Puisque $K[T]$ est principal, on a bien que $ker(f)$ est engendré par un élément : si l'on impose que le coefficient au plus haut degré vaut 1, le choix de P est unique.

Exemples

1. $T \in K(T)$ est transcendant ;
2. i est algébrique sur $\mathbb{Q}$ avec le polynôme minimal $x^2 + 1$;
3. $\pi \in \mathbb{C}$ est transcendant sur $\mathbb{Q}$.

Proposition 3.1.7. *Soient L/K une extension de corps et $\alpha \in K$. Les assertions suivantes sont équivalentes*

(i) α est algébrique sur K ;
(ii) $K[\alpha] = K(\alpha)$;
(iii) $K[\alpha]$ est un K-espace vectoriel de dimension finie.

Si une (et donc toutes) de ces conditions est satisfaite, alors $[K[\alpha] : K]$ *est le degré de polynôme minimal de* α*, on l'appelle le degré de* α *sur* K*.*

Démonstration. $(i) \Rightarrow (ii)$: en effet $K[\alpha] \simeq K[T]/P$ avec P irréductible, donc $K[\alpha]$ est un corps et on a bien $K[\alpha] = K(\alpha)$.

$(ii) \Rightarrow (i)$: si α est transcendant, alors $K[\alpha]$ est isomorphe à $K[T]$ qui n'est pas un corps.

$(i) \Rightarrow (iii)$: si P est le polynôme minimal de α, alors le K-espace vectoriel $K[\alpha]$ est isomorphe à $K[T]/P$ qui est de dimension finie.

$(iii) \Rightarrow (i)$: si α est transcendant, le K-espace vectoriel $K[\alpha]$ est isomorphe à $K[T]$ qui est de dimension infinie. □

Définition 3.1.8. Une extension de corps L/K est *algébrique* si tout élément de L est algébrique sur K.

En particulier, toute extension finie est algébrique, on peut aussi avoir des extensions algébriques infinies :

Théorème 3.1.9. *Soit* L/K *une extension de corps. Soit* F *l'ensemble des éléments de* L *qui sont algébriques sur* K*. Alors*

- F *est un sous-corps de* L *;*
- *tout élément de* F *qui est algébrique sur* F *est dans* F *;*
- *si* L *est algébriquement clos,* F *est algébriquement clos : on dit que* F *est une clôture algébrique de* K*.*

Remarque. Rappelons qu'un corps L est algébriquement clos si tout polynôme à coefficients dans L admet une racine dans L. On dit qu'une extension $\bar{K}/K$ est une clôture algébrique si $\bar{K}$ est algébriquement clos et l'extension $\bar{K}/K$ est algébrique. Le théorème précédent montre qu'une telle extension existe s'il existe une extension L de K qui est algébriquement close : ce qui est toujours vrai en utilisant le lemme de Zorn. Par exemple, l'ensemble $\bar{\mathbb{Q}}$ de nombres complexes algébriques sur $\mathbb{Q}$ est un corps algébriquement clos : c'est une clôture algébrique de $\mathbb{Q}$.

Démonstration. On a $K \subset F$. Si $x \in L$ est algébrique sur K, alors il existe un polynôme unitaire $X^n + \ldots + a_0$ dans $K[X]$ qui admet x comme racine. Alors $(-1)^n X^n + \ldots + a_0$ annule $-x$ et $1 + \ldots + a_0 X^n$ annule x^{-1}, d'où $-x$ et x^{-1} sont algébriques sur K. Montrons que si x, y sont dans F, alors $x + y$ et xy sont dans F : on a que $K[x] = K(x)$ est un corps par 3.1.7 et y est algébrique sur K (et donc sur le corps $K[x]$), d'où $K[x, y] = K[x][y]$ est de dimension finie sur $K[x]$, et donc aussi sur K par proposition 3.1.3. Comme $K[x, y]$ contient $K[x + y]$ et $K[xy]$, ces espaces vectoriels sont de dimension finie sur K, donc $x + y$ et xy sont dans F. On a donc montŕe que F est un sous-corps de L.

Soit $x \in L$ algébrique sur F. Alors il existe un polynôme unitaire $P = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ de $F[X]$ qui annule x. On a que chaque a_i est algébrique sur K, on a par récurrence que $K[a_0, \ldots a_{n-1}] = K(a_0, \ldots a_{n-1})$ est un corps K' de

dimension finie sur K. Comme $P \in K'[X]$ est non nul et annule x, on obtient que x est algébrique sur K', i.e. $K'[x]$ est de dimension finie sur K' : on a donc que $K'[x]$ est de dimension finie sur K, i.e. x est algébrique sur K, donc $x \in F$.

Si maintenant $P \in F[X]$ non constant, il a une racine x dans le corps algébriquement clos L, mais x est alors algébrique sur F d'où $x \in F$. □

Définition 3.1.10. Soit P un polynôme irréductible de $K[X]$. On dit qu'une extension L/K est un corps de *rupture* pour P sur K s'il existe une racine α de P dans L telle que $L = K[\alpha]$. Une extension L/K est un corps de *décomposition* pour P sur K si P est scindé sur L (i.e. toutes les racines de P sont dans L) et si L est engendré par les racines de P sur L.

Exemples

1. $\mathbb{C}$ est le corps de rupture (et de décomposition) de $x^2 + 1$;
2. $\mathbb{Q}(\sqrt[3]{2})$ est le corps de rupture de $x^3 - 2$ sur $\mathbb{Q}$, mais ce n'est pas le corps de décomposition de ce polynôme.

Théorème 3.1.11. *Pour tout polynôme irréductible $P \in K[X]$ il existe un corps de rupture L, unique à K-isomorphisme près.*

Démonstration. Puisque P est irréductible, $L = K[X]/P$ est un corps, une extension de K : l'application $K \to L$, $a \mapsto \bar{a}$ est injective. La classe $\bar{X}$ de X dans L est bien une racine de P, donc L est un corps de rupture de P.

Soit L' un corps de rupture pour P sur K : $L' = K[\alpha']$ et $P(\alpha') = 0$. Alors l'application $K[X] \to L', Q \mapsto Q(\alpha')$ est surjective, de noyau (P) : on obtient donc un K-isomorphisme entre $L = K[X]/P$ et L'. □

Théorème 3.1.12. *Pour tout polynôme $P \in K[X]$ il existe un corps de décomposition L, unique à K-isomorphisme près.*

Démonstration. Pour l'existence on procède par récurrence sur $deg\, P$: on a immédiatement le cas $deg\, P \leq 1$. Soit Q un facteur irréductible de P. Alors Q admet un corps de rupture $K' = K(\alpha)$ d'après le théorème précédent. On a donc $P = (X - \alpha)P'$ dans $K'[X]$. Par récurrence, il existe un corps de décomposition L pour P' : $P = (X - \alpha)P'$ est donc aussi scindé sur L et d'autre part $L = K'(\alpha_2, \ldots \alpha_n)$ où $\alpha_2, \ldots \alpha_n$ sont des racines de P i.e. c'est un corps de décomposition de P sur K.

Pour l'unicité on applique le lemme ci-dessous à $K = K'$ et $f = Id$. □

Lemme 3.1.13. *Soit $f : K \to K'$ un isomorphisme de corps, P un polynôme de $K[X]$ et L, L' des corps de décomposition de P sur K et K'. Alors il existe un isomorphisme de corps $f' : L \to L'$ qui prolonge f.*

Démonstration. Si P est scindé, on a $L = K$, $L' = K'$ et l'assertion est immédiate. Sinon, soit α une racine de P dans $L \setminus K$, de polynôme minimal $Q \in K[X]$. Alors $f(Q)$ admet une racine α' dans L' et $K[\alpha], K[\alpha']$ sont des corps de rupture respectifs de Q, $f(Q)$ sur K et K', on a un isomorphisme $f_1 : K[\alpha] \to K[\alpha']$, $\alpha \mapsto \alpha'$. On termine la preuve par récurrence. □

3.2 Corps finis

On s'intéresse dans cette section aux corps K dont l'ensemble sous-jacent est fini. Rappelons qu'on appelle la *caractérisque* d'un corps K le plus petit entier n (s'il existe) tel que $n \cdot 1 = 0$ dans K. Si un tel entier n'existe pas, on dit que K est de caractéristique 0.

3.2.1 Construction

Théorème 3.2.1. *1. La caractéristique d'un corps fini K est un nombre premier p ; si $d = [K : \mathbb{F}_p]$, le nombre d'éléments de K est p^d.*

2. Soit $q = p^d$ où p est un nombre premier et $d > 0$ un entier. Alors il existe un corps de cardinal q, unique à isomorphisme près : c'est le corps de décomposition sur $\mathbb{F}_p$ du polynôme $X^q - X$, on le note $\mathbb{F}_q$.

Démonstration. 1. Soit $\phi : \mathbb{Z} \to K, n \mapsto n \cdot 1$ l'homomorphisme d'anneaux. Le noyau $ker(\phi)$ est un idéal premier non nul (car K est fini) de $\mathbb{Z}$: l'anneau quotient $\mathbb{Z}/ker(\phi)$ est isomorphe à un sous-anneau de K, donc intègre. On a donc qur $ker(\phi) = (p)$ pour p premier.

2. Soit K le corps de décomposition sur $\mathbb{F}_p$ du polynôme $X^q - X$. Notons que l'ensemble K' de ses racines est deja un corps car $(x + y)^{p^d} = x^{p^d} + y^{p^d}$ d'après le lemme ci-dessous. Par définition d'un corps de décomposition, on a $K = K'$. Par ailleurs, les racines de $X^q - X$ sont simples (la dérivée de ce polynôme vaut -1), et donc le cardinal de K' est q.

   Si L est un corps de cardinal q, alors tout élément x de L vérifie $x^q = x$ (on a $x^{q-1} = 1$ pour tout $x \neq 0$ car L^* est un groupe de cardinal $q - 1$). Ainsi $X^q - X$ est scindé sur L et L contient donc le corps de décomposition de $X^q - X$, par cardinalité, L est isomorphe à ce dernier. □

Lemme 3.2.2. *Soit K un corps de caractéristique p. Pour $x, y \in K$, on a $(x+y)^{p^n} = x^{p^n} + y^{p^n}$.*

Démonstration. laissée en exercice (utiliser la récurrence). □

Exemple. On a $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$, $\mathbb{F}_8 = \mathbb{F}_2[X]/(X^3 + X + 1)$, $\mathbb{F}_9 = \mathbb{F}_3[X]/(X^2 + 1)$. Pour montrer que l'on peut faire apparaître tous les corps finis de caractéristique p comme corps de rupture sur $\mathbb{F}_p$ on a besoin de savoir qu'il y a des

polynômes irréductibles de tout degré sur $\mathbb{F}_p$, ce qui sera démontré dans le cours plus avancé ('Corps finis II').

Exercice. Montrer qu'on a $\bar{\mathbb{F}_p} = \bigcup_{d\geq 0} \mathbb{F}_{p^d}$ pour la clôture algébrique d'un corps fini $\mathbb{F}_p$.

3.2.2 Frobenius, norme et trace

Proposition 3.2.3. *Soit $\mathbb{F}$ un corps fini de caractéristique p, alors*

$$Frob_p : \mathbb{F} \to \mathbb{F}, x \mapsto x^p$$

est un automorphisme, dit **de Frobenius** *de $\mathbb{F}$.*

Démonstration. D'après le lemme 3.2.2, on a que $Frob_p$ est bien un homomorphisme. De plus, il est injectif : $x^p = 0$ implique $x = 0$, il est donc aussi surjectif par un argument de cardinalité. □

On peut étendre le morphisme de Frobenius sur la clôture algébrique $\bar{\mathbb{F}}$ de $\mathbb{F}_p$. On note $Frob_{p^s}$ l'automorphisme de Frobenius itéré s fois. Si $\alpha \in \bar{\mathbb{F}}$, alors il existe s minimal tel que $Frob_{p^s}(\alpha) = \alpha$ (ce qui est équivalent à dire que $\alpha \in \mathbb{F}_{p^s}$.) On appelle alors $Frob_{p^i}(\alpha), 1 \leq i < s$ les *conjugués* de α.

Si α un élément primitif de $\mathbb{F}_q$, i.e. si α engendre le groupe $\mathbb{F}_q^*$, alors les puissances α^i, $0 < i \leq q-1$ parcourrent tous les éléments de $\mathbb{F}_q^*$, on a donc lécalité

$$X^{q-1} - 1 = \prod_{i=1}^{q-1}(X - \alpha^i). \tag{3.1}$$

Si $\mathbb{F}_q$ est un corps fini et si $K/\mathbb{F}_q$ une extension finie de degré d et $\alpha \in K$ on a la *la norme* de α : $N_{K/\mathbb{F}_q} = \prod_{i=0}^{d-1} Frob_{q^i}(\alpha) = \alpha^{(q^d-1)/(q-1)}$ et *la trace* de α : $Tr_{K/\mathbb{F}_q} = \sum_{i=0}^{d-1} Frob_{q^i}(\alpha)$.

La norme $N_{K/\mathbb{F}_q}$ induit un homomorphisme surjectif de K^* dans $\mathbb{F}_q^*$. La trace $Tr_{K/\mathbb{F}_q}$ induit un morphisme surjectif $\mathbb{F}_q$-linéaire de K^* à $\mathbb{F}_q^*$.

3.2.3 L'anneau $\mathbb{Z}/n\mathbb{Z}$

Dans cette section on s'intéresse à des propriétés de structure de l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$.

Notons que

$$(\mathbb{Z}/n\mathbb{Z})^* = \{\bar{x}, x \in \mathbb{Z}, x \text{ et premier avec } n\}$$

est muni d'une structure de groupe multiplicative.

Définition 3.2.4. L'indicatrice d'Euler est une fonction $\phi : \mathbb{N} \to \mathbb{N}$ définie par $\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*$.

Théorème 3.2.5 (restes chinois)**.** *Soient $m, n \in \mathbb{Z}$ premiers entre eux. Alors l'application*

$$\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

qui envoie la classe de x modulo mn sur les classes modulo m et modulo n, est un isomorphisme d'anneaux.

Démonstration. On considère l'homomorphisme $f : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, $x \mapsto (x + m\mathbb{Z}, x + n\mathbb{Z})$ qui associe à x les classes modulo m et modulo n. Comme m et n sont premiers entre eux, $ker(f) = mn\mathbb{Z}$. D'après la proposition 2.1.7, on a donc bien un morphisme injectif d'anneaux $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ comme dans l'énoncé. Puisqu'il s'agit des anneaux finis de même cardinal, c'est aussi un morphisme surjectif. □

Corollaire 3.2.6. *Soient $m, n \in \mathbb{Z}$ premiers entre eux. Alors on a un isomorphisme de groupes*

$$(\mathbb{Z}/mn\mathbb{Z})^* \to (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*.$$

En particulier, $\phi(mn) = \phi(m)\phi(n)$: l'indicatrice d'Euler est une fonction arithmétique multiplicative.

Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ est une décomposition en facteurs premiers, on a en particulier

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \mathbb{Z}/p_2^{\alpha_2}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_m^{\alpha_m}\mathbb{Z} \tag{3.2}$$

et

$$(\mathbb{Z}/n\mathbb{Z})^* \simeq (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^* \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z})^* \times \ldots \times (\mathbb{Z}/p_m^{\alpha_m}\mathbb{Z})^*. \tag{3.3}$$

Par définition on voit facilement que $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$. On a donc

$$\phi(n) = \prod_{i=1}^{m} p_i^{\alpha_i} - p_i^{\alpha_i - 1} = n \prod_{i=1}^{m} (1 - \frac{1}{p_i}). \tag{3.4}$$

Proposition 3.2.7. *Soit n un entier. Pour chaque entier $d \,|\, n, d \geq 1$ il existe un unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d : c'est le sous-groupe cyclique engendré par la classe de n/d dans $\mathbb{Z}/n\mathbb{Z}$.*

Démonstration. On écrit $n = dq$. On a alors que $\bar{q}$ est d'ordre d dans $\mathbb{Z}/n\mathbb{Z} : r\bar{q} = \overline{rq}$, donc si $r\bar{q} = 0$, alors rq est divisible par $n = dq$ et donc r est divisible par d.

Soit $H \subset \mathbb{Z}/n\mathbb{Z}$ un sous-groupe d'ordre d. Si $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est une surjection canonique, on a $s^{-1}(H) = m\mathbb{Z}$. Ainsi H est engendré par $\bar{m}$. Puisque $d\bar{m} = 0$ on déduit comme ci-dessus que q divise m, d'où H est contenu dans le sous-groupe engendré par $\bar{m}$ et donc égal à ce sous-groupe. □

Corollaire 3.2.8. *Pour tout entier n on a $n = \sum_{d \,|\, n} \phi(d)$.*

Démonstration. On peut écrire $\mathbb{Z}/n\mathbb{Z}$ comme union disjointe des ensembles $H_d := \{x \in \mathbb{Z}/n\mathbb{Z} \text{ d'ordre } d\}$. D'après la proposition précédente, le cardinal de H_d est le nombre de générateurs de $\mathbb{Z}/d\mathbb{Z}$, et il est donc égal à $\phi(d)$. Or le cardinal de $\mathbb{Z}/n\mathbb{Z}$ est n, on obtient la formule voulue. □

Théorème 3.2.9 (Petit théorème de Fermat)**.** *Pour p premier et $(a,p) = 1$ on a $a^{p-1} \equiv 1 (mod\ p)$.*

Démonstration. Notons que pour $1 \leq i, j \leq (p-1)$ différents, les classes de ai et aj dans $\mathbb{Z}/p\mathbb{Z}$ sont différents : si $\overline{ai} = \overline{aj}$ alors $p \,|\, a(i-j)$, contradiction. Ainsi $\prod ai \equiv 1 \cdot 2 \ldots (p-1) \bmod p$, d'où $a^{p-1} \equiv 1 \bmod p$. □

Dans le cas général, on a l'énoncé suivant

Théorème 3.2.10 (Théorème d'Euler)**.** *Pour n un entier et $(a,n) = 1$ on a $a^{\phi(n)} \equiv 1 (mod\ n)$.*

Exercice. Démontrer ce théorème (on peut utiliser la même approche que pour le théorème de Fermat, en remplaçant les entiers $1 \ldots (p-1)$ par les entiers premiers à n.)

Théorème 3.2.11. *Le groupe des éléments inversibles d'un corps fini $\mathbb{F}_q$ est cyclique. Plus généralement, tout sous-groupe de $\mathbb{F}_q^*$ est cyclique.*

Démonstration. Soit $G \subset \mathbb{F}_q^*$ et soit n le cardinal de G. On a alors d'après le corollaire 3.2.8

$$n = \sum_{d \,|\, n} \phi(d), \tag{3.5}$$

où $\phi(d)$ est le nombre d'éléments d'ordre d dans $\mathbb{Z}/d\mathbb{Z}$. Par ailleurs, si $x \in G$ est d'ordre d, alors on a une équation $x^d - 1 = 0$ dans le corps $\mathbb{F}_q$, ainsi on a au plus $\phi(d)$ éléments d'ordre d dans $\mathbb{F}_q^*$. L'égalité (3.5) implique alors qu'on a exactement $\phi(d)$ éléments d'ordre d dans $\mathbb{F}_q^*$. En particulier, on a donc un élément d'ordre n et le groupe G est cyclique. □

Exercice. Soit $\mathbb{F}_q$ un corps fini et soit K une extension finie de $\mathbb{F}_q$. Montrer qu'il existe $\alpha \in K$ tel que $K = \mathbb{F}_q(\alpha)$.

Théorème 3.2.12. *Soit p premier et $\alpha \geq 1$.*

- *Si p est impair, $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ est un groupe cyclique.*
- *Si $p = 2$ et $\alpha \geq 3$, alors $(\mathbb{Z}/2^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/2^{\alpha-1}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ n'est pas cyclique. Les groupes $(\mathbb{Z}/2\mathbb{Z})^* = 1$ et $(\mathbb{Z}/4\mathbb{Z})^* = \mathbb{Z}/2\mathbb{Z}$ sont cycliques.*

Démonstration. Supposons d'abord p impair. Le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique d'après le théorème 3.2.11. Soit $x \in \mathbb{Z}$ tel que x modulo p engendre $(\mathbb{Z}/p\mathbb{Z})^*$. On a alors que $\bar{x} \in (\mathbb{Z}/p^\alpha\mathbb{Z})^*$ est d'ordre $m(p-1)$ pour certain m, ainsi $y = \bar{x}^m$ est d'ordre exactement $(p-1)$. D'après le lemme 3.2.13 ci-dessous, $\overline{p+1}$ est d'ordre $p^{\alpha-1}$. Comme $p-1$ et $p^{\alpha-1}$ sont premiers entre eux, l'ordre de $y\overline{(p+1)}$ est exactement $(p-1)p^{\alpha-1}$ et donc $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ est cyclique.

Dans le cas $p = 2$ et $\alpha \geq 3$ (les cas $\alpha = 1$ et $\alpha = 2$ sont immédiats) on utilise le lemme (3.2.14) ci-dessous : 5 est d'ordre $2^{\alpha-2}$ et -1 (d'ordre 2) n'appartient pas au sous-groupe engendré par 5. Comme le cardinal de $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ est $2^{\alpha-1}$, on obtient bien que $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ est le produit direct de groupes engendrés par 5 et par -1, i.e. $(\mathbb{Z}/2^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/2^{\alpha-1}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. □

Lemme 3.2.13. *Pour p un premier impair, la classe de $p+1$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ est d'ordre $p^{\alpha-1}$.*

Démonstration. Montrons par récurrence que

$$(p+1)^{p^k} \equiv 1 + p^{k+1} \bmod p^{k+2}. \tag{3.6}$$

Pour $k = 0$ c'est immédiat, pour $k = 1$ on a $(p+1)^p \equiv 1 + C_p^1 p + C_p^2 p^2 \equiv 1 + p^2 + p^3(p-1)/2 \bmod p^3$ ce qui est congru à $1 + p^2$ si p est impair. Supposons maintenant $(p+1)^{p^{k-1}} = 1 + p^k + ap^{k+1}$. On a $(p+1)^{p^k} = (1 + p^k + ap^{k+1})^p \equiv 1 + p^{k+1} \bmod p^{k+2}$. En particulier $(p+1)^{p^{\alpha-1}} \equiv 1 \bmod p^\alpha$, mais $(p+1)^{p^{\alpha-2}} \equiv 1 + p^{\alpha-1}$ n'est pas congru à 1 mod p^α . □

Lemme 3.2.14. *Soit $\alpha \geq 3$. La classe de 5 est d'ordre $2^{\alpha-2}$ dans $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ et -1 (d'ordre 2) n'appartient pas au sous-groupe engendré par 5.*

Démonstration. Montrons par récurrence que

$$5^{2^k} \equiv 1 + 2^{k+2} \bmod 2^{k+3}. \tag{3.7}$$

On le vérifie immédiatement pour $k = 0$, pour $k = 1 : 25 \equiv 9 \bmod 2^4$. Supposons $5^{2^{k-1}} = 1 + 2^{k+1} + a2^{k+2}$. On a alors $5^{2^k} = (1 + 2^{k+1} + a2^{k+2})^2 = 1 + 2^{k+2} \bmod 2^{k+3}$. On a donc en particulier $5^{2^{\alpha-2}} \equiv 1 \bmod 2^\alpha$ mais $5^{2^{\alpha-3}} \equiv 1 + 2^{\alpha-1} \bmod 2^\alpha$, donc 5 est bien d'ordre $2^{\alpha-2}$. Pour la deuxième assertion il suffit de noter que pour tout m entier on a $5^m \equiv 1$ (et pas -1) mod 4. □

3.3 Polynômes irréductibles

Dans cette section on s'intéresse aux critères d'irréducibilité des polynômes dans $\mathbb{Q}[x]$, $\mathbb{Z}[x]$ et dans un corps fini.

On dispose d'un morphisme de réduction $\mathbb{Z}[x] \to \mathbb{F}_p[x]$,

$$P(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_0 \mapsto \bar{P}(x) = \bar{a}_d x^d + \bar{a}_{d-1}x^{d-1} + \ldots + \bar{a}_0$$

où $\bar{a}_i$ est la classe de a_i dans $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.
On vérifie immédiatement que $\overline{PQ} = \bar{P} \cdot \bar{Q}$ et $\overline{P+Q} = \bar{P} + \bar{Q}$ (i.e. le morphisme de réduction est un morphisme d'anneaux).

Définition 3.3.1. Soit $P \in \mathbb{Z}[x]$. Le *contenu* $c(P)$ est le plus grand diviseur commun de tous les coéfficients. Si $c(P) = 1$, on dit que P est primitif.

Lemme 3.3.2 (Gauss)**.** *Soient $P, Q \in \mathbb{Z}[x]$. Alors $c(PQ) = c(P)c(Q)$, à une multiplication par un élément inversible près.*

Démonstration. laissée en exercice. □

Corollaire 3.3.3. *Soit $P \in \mathbb{Z}[x]$. Si P est irréductible dans $\mathbb{Z}[x]$, alors P est irréductible dans $\mathbb{Q}[x]$.*

Démonstration. Supposons que P n'est pas irréductible dans $\mathbb{Q}[x]$. On a alors $aP = Q \cdot R$ avec $a \in \mathbb{Z}, Q, R \in \mathbb{Z}[x]$. D'après le lemme précédent, $a \cdot c(P) = c(Q)c(R)$, en particulier, on peut écrire $a = a_1 a_2$ avec $a_1 \mid c(Q)$ et $a_2 \mid c(R)$, d'où $P = \frac{Q}{a_1} \cdot \frac{R}{a_2}$ une factorization dans $\mathbb{Z}[x]$, contradiction. □

Proposition 3.3.4 (Critère d'Eisenstein)**.** *Soit $P(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_0 \in \mathbb{Z}[x]$. Supposons qu'il existe p premier tel que*

- *p divise a_i, $0 \leq i < d-1$ mais p ne divise pas a_d ;*
- *p^2 ne divise pas a_0.*

Alors $P(x)$ est irréductible dans $\mathbb{Q}[x]$.

Démonstration. Supposons le contraire. D'après le corollaire 3.3.3, on peut alors écrire $P = B \cdot C$ avec $B(x) = b_n x^n + b_{n-1}x^{n-1} + \ldots + b_0 \in \mathbb{Z}[x]$ et $C(x) = c_m x^m + c_{m-1}x^{m-1} + \ldots + c_0 \in \mathbb{Z}[x]$. On a en particulier $d = m + n$, $a_d = b_n c_m$ et $a_0 = c_0 b_0$. On a donc dans $\mathbb{Z}/p\mathbb{Z}[x]$: $\bar{a}_d x^d = \bar{P} = \bar{B} \cdot \bar{C}$ avec $\bar{a}_d \neq 0$, d'où $\bar{B} = x^n$ et $\bar{C} = x^m$ à multiplication par une constante près. On obtient donc que p^2 divise a_0, contradiction. □

Remarque. Ce critère reste vrai en remplaçant $\mathbb{Z}$ par un anneau factoriel.

Proposition 3.3.5. *Soit $P(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_0 \in \mathbb{Z}[x]$. Soit p un nombre premier tel que p ne divise pas a_n. Alors, si la réduction $\bar{P}$ de P dans $\mathbb{Z}/p\mathbb{Z}$ est irréductible, alors P est irréductible sur $\mathbb{Q}$.*

Démonstration. Supposons le contraire. D'après 3.3.3, on a alors $P = QR$ dans $\mathbb{Z}[x]$. Puisque p ne divise pas a_n, $\bar{P}$ a le même degré que P et $\bar{Q}$ et $\bar{R}$ sont non constants, contradiction. □

Proposition 3.3.6. *Soit K un corps et soit $P \in K[X]$. Si P n'a pas de racines dans toute extension de K de degré au plus $n/2$, alors P est irréductible.*

Démonstration. Si P n'est pas irréductible, on peut écrire $P = Q \cdot R$, i.e. un des facteurs irréductibles de P est donc de degré $0 < d \leq n/2$, il a donc une racine dans son corps de rupture qui est une extension de degré d de K, contradiction. □

Exercice. Montrer que $X^4 + X + 1$ est irrédictible sur $\mathbb{F}_2$.

On s'intéresse ensuite à l'irréducibilité des polynômes cyclotomiques.

Soit $\mu_n \subset \mathbb{C}^*$ les racines n-ièmes de l'unités, on voit μ_n comme groupe multiplicatif. On note μ_n^* l'ensemble des racines *primitives* n-ièmes de l'unité, i.e. $\mu_n^* = \{e^{2ik\pi/n} \,|\, (k,n) = 1\}$ est formé des générateurs de $(\mu_n, \times)$. Le cardinal de μ_n^* est $\phi(n)$.

Définition 3.3.7. Le n-ième *polynôme cyclotomique* est le polynôme

$$\Phi_n = \prod_{\xi \in \mu_n^*} (x - \xi).$$

Proposition 3.3.8. *On a $x^n - 1 = \prod_{d \,|\, n} \Phi_d$. Pour tout $n \in \mathbb{N}^*$, le polynôme Φ_n est dans $\mathbb{Z}[x]$.*

Démonstration. Pour montrer que $x^n - 1 = \prod_{d \,|\, n} \Phi_d$ il suffit de remarquer que ce sont deux polynômes unitaires, scindés et à racines simples dans $\mathbb{C}[x]$, qui ont les mêmes racines. Pour montrer la deuxième assertion, on procède par récurrence sur n : pour $n = 1$, on a $\Phi_1 = x - 1$; si tous les Φ_d sont dans $\mathbb{Z}[x]$ pour $d < n$, on a $x^n - 1 = R \cdot \Phi_n$ avec $R \in \mathbb{Z}[x]$ unitaire, on a donc Φ_n est aussi dans $\mathbb{Z}[x]$ et unitaire (par la division euclidienne). □

Théorème 3.3.9. *Le polynôme Φ_n est irréductible sur $\mathbb{Q}$.*

Démonstration. Soit ξ une racine primitive n-ième de l'unité. Soit f le polynôme minimal de ξ sur $\mathbb{Q}$. Si ξ' est un autre élément de μ_n^*, on peut écrire $\xi' = \xi^m$ avec m premier à n. On a donc $m = \prod_{i=1}^r p_i^{\alpha_i}$ où les nombres premiers p_i ne divisent pas n. D'après le lemme ci-dessous, le polynôme minimal de ξ' sur $\mathbb{Q}$ est encore f. On obtient ainsi que f est divisible dans $\mathbb{C}[x]$ par tous les $x - \xi'$ avec $\xi' \in \mu_n^*$, donc f est divisible par Φ_n (dans $\mathbb{C}[x]$, donc aussi dans $\mathbb{Q}[x]$). Comme $\Phi_n(\xi) = 0$, Φ_n est multiple de f et donc $\Phi_n = f$, donc Φ_n est irréductible sur $\mathbb{Q}$. □

Lemme 3.3.10. *Soit $\xi \in \mu_n^*$ et soit p un nombre premier ne divisant pas n. Soient f, g les polynômes minimaux respectifs de ξ, ξ^p sur $\mathbb{Q}$. Alors $f = g$ sont dans $\mathbb{Z}[x]$.*

Démonstration. Montrons que f est à coefficients dans $\mathbb{Z}[x]$, la preuve pour g est similaire. On a que $x^n - 1$ annule ξ et donc f divise $x^n - 1$. Comme $\mathbb{Z}[x]$ est factoriel, on peut décomposer $x^n - 1$ en produit de facteurs irréductibles $P_1 \dots P_r$ dans $\mathbb{Z}[x]$, on peut de plus les supposer unitaires de sorte qu'on a que $P_1, \dots, P_r$ sont encore des facteurs irréductibles dans $\mathbb{Q}[x]$, donc f est l'un des P_i et $f \in \mathbb{Z}[x]$.

Montrons maintenant que $f = g$. Supposons le contraire. Alors f et g sont premiers entre eux et divisent Φ_n, donc fg divise Φ_n. Par ailleurs, $h = g(x^p)$ annule ξ, il est donc divisible par f. Ainsi la réduction $\bar{h}$ modulo p est divisible par $\bar{f}$ dans $\mathbb{Z}/p\mathbb{Z}[x]$. Puisque tout élément $\bar{a}$ de $\mathbb{F}_p$ vérifie $\bar{a}^p = \bar{a}$, on obtient $\bar{h} = \bar{g}^p$. Ainsi $\bar{f}$ divise $\bar{g}^p$. Le polynôme unitaire $\bar{f}$ n'est pas forcement irréductible dans $\mathbb{Z}/p\mathbb{Z}[x]$, mais il admet un facteur irréductible ϕ et on a donc $\phi \,|\, \bar{g}$. Par ailleurs, $\bar{f}\bar{g}$ divise Φ_n, on obtient a fortiori que ϕ^2 divise le polynôme $Q = x^n - 1$ dans $\mathbb{Z}/p\mathbb{Z}[x]$, ce qui n'est pas possible car Q est premier avec $Q' : x/\bar{n}Q' - Q = 1$ ($\bar{n}$ est inversible dans $\mathbb{Z}/p\mathbb{Z}$.) □

On s'intéresse maintenant aux propriétés des polynômes cyclotomique sur un corps fini.

Proposition 3.3.11. *Soit $\mathbb{F}_q$ un corps fini avec $q = p^s$ éléments et soit n premier à p. Alors $\Phi_n(x)$ est un produit de facteurs irréductibles dans $\mathbb{F}_q$, chacun de degré ℓ où ℓ est l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^*$.*

Démonstration. Pour α une racine de $\Phi_n(x)$ dans $\bar{\mathbb{F}}_q$, on a alors que ℓ est minimal tel que $\alpha^{q^\ell} = \alpha$. On a donc que $Frob_i(\alpha), i \leq \ell$ sont aussi des racines de Φ_n et $\prod_{i=0}^{\ell-1}(x - Frob_{q^i}) = \prod_{i=0}^{\ell-1}(x - \alpha^{q^i})$ est un facteur de Φ_n, d'où le résultat. □

Corollaire 3.3.12. *Le polynôme $\Phi_n(x)$ est scindé complément dans $\mathbb{F}_q[x]$ si et seulement si $q \equiv 1$ mod n.*

Corollaire 3.3.13. *Les conditions suivantes sont équivalentes :*
(i) Le polynôme $\Phi_n(x)$ est irréducible dans $\mathbb{F}_q[x]$;
(ii) q est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z})^*$.

3.4 Problèmes

1. Montrer que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.
2. Soit $P(X) = X^3 + 3X - 2$ dans $\mathbb{Q}[X]$.
   (a) Montrer que $\mathbb{Q}[X]/(P)$ est un corps.
   (b) Est-il isomorphe à un sous-corps de $\mathbb{R}$?
   (c) Est-il isomorphe à un sous-corps de $\mathbb{C}$ non contenu dans $\mathbb{R}$?

(d) Combient P a-t-il racines dans $\mathbb{Q}[X]/(P)$?

(e) Notons x la classe de X dans $\mathbb{Q}[X]/(P)$. Montrer que $\{1, x, x^2\}$ est une $\mathbb{Q}$-base de $\mathbb{Q}[X]/(P)$.

(f) Exprimer $(2x^2 + x - 3)(3x^2 - 4x + 1)$ and $(x^2 - x + 4)^{-1}$ dans cette base.

3. (**théorème d'un élément primitif**) Soit K un corps de caractéristique zéro et soit $L = K(x, y_1, \dots y_n)$ une extension finie de K. On va montrer qu'il existe $z \in L$ tel que $L = K(z)$:

(a) Supposons d'abord $n = 1$. Soit P le polynôme minimal de x sur K et soit Q celui de y_1. Soit $P(X) = \prod_{i=1}^{r}(X - \alpha_i)$, $Q(X) = \prod_{j=1}^{s}(X - \beta_j)$ les décompositions de P et Q dans leurs corps de décomposition.

i. Montrer que les α_i (resp. les β_j) sont tous distincts.

ii. Montrer qu'on peut trouver $t \in K$ distincts de tous les $\frac{x-\alpha_i}{\beta_j - y_1}$ pour tout i et $j \neq 1$.

iii. Soit $z = x + ty_1 \in L$. Montrer que le pgcd de Q et $P(z - tX) \in K(z)[X]$ est $X - y_1$. En déduire que y_1 et x sont dans $K(z)$ et puis que $L = K(z)$.

(b) Conlure par récurrence.

4. Montrer les isomorphismes suivant et donner un générateur du groupe des inversibles des corps en question :

(a) $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/(X^2 + X + 1)$;

(b) $\mathbb{F}_8 \simeq \mathbb{F}_2[X]/(X^3 + X + 1)$;

(c) $\mathbb{F}_{16} \simeq \mathbb{F}_2[X]/(X^4 + X + 1)$;

(d) $\mathbb{F}_9 \simeq \mathbb{F}_3[X]/(X^2 + X - 1)$.

5. Soient $\mathbb{F}_q$ un corps fini à q éléments, K une extension de $\mathbb{F}_q$ et f un élément de $K[X]$. Montrer que $f \in \mathbb{F}_q[X]$ si et seulement si $f(X)^q = f(X^q)$.

6. (a) Soit p un nombre premier. Montrer que $P(X) = X^{p-1} + \ldots + X + 1$ est irréductible sur $\mathbb{Q}$ (Indication : considérer $P(X + 1)$).

(b) Montrer que $X^n - 2$ est irréductible sur $\mathbb{Q}$ et sur $\mathbb{Z}$.

7. Pour $\mathbb{F}_q$ un corps fini de caractéristique p on note

$$\mathbb{F}_q^2 = \{x \in \mathbb{F}_q \mid \exists y \in \mathbb{F}_q, x = y^2\}.$$

(a) Montrer que si $p = 2$ alors $\mathbb{F}_q^2 = \mathbb{F}_q$.

(b) Pour $p > 2$ montrer que $|\mathbb{F}_q^2| = \frac{q+1}{2}$.

(c) Pour $p > 2$ montrer que $x \in \mathbb{F}_q^2 \Leftrightarrow x = 0$ ou $x^{q-1/2} = 1$.

(d) En déduire que pour $p > 2$ on a -1 est un carré dans $\mathbb{F}_q$ si et seulement si q est congru à 1 modulo 4.

8. Montrer que le polynôme $P(X) = X^5 + X^2 + X + 2$ est irréductible sur $\mathbb{Z}$:

(a) Factoriser $\overline{P(X)}$ dans $\mathbb{F}_2[X]$ (indication : utiliser que $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$). En déduire que si P n'est pas irréductible sur $\mathbb{Z}$, alors il a une racine dans $\mathbb{Z}$.

(b) Conclure (par exemple, montrer que la reduction de P dans $\mathbb{F}_3[X]$ n'a pas de racines).

Chapitre 4

Introduction à la cryptographie

Dans cette partie on décrit deux ascpects de la cryptographie moderne, qui utilise le contenu de ce cours : le système de chiffrement RSA (qui utilise l'arithméque dans l'anneau $\mathbb{Z}/n\mathbb{Z}$) et les codes correcteurs d'erreurs (qui utilisent des propriétés des corps finis).

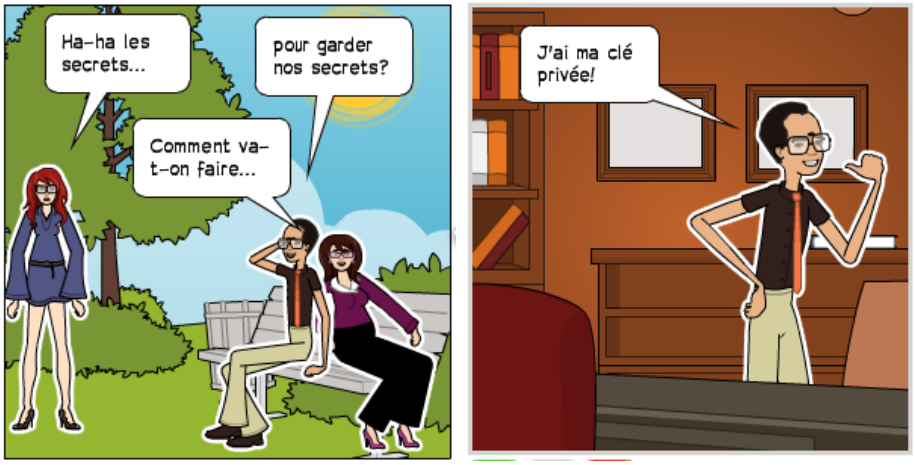
4.1 Systèmes de chiffrement à clé publique

On considère généralement le contexte suivant pour les systèmes cryptographiques à clé publique : deux personnes, Alice et Bob veulent s'échanger des messages de façon sécurisée. Eva veut lire leurs messages, elle a l'accès au canal public de la transmission des messages d'Alice et Bob. Dans ce système, on distingue trois algorithmes de base : l'échange de clés, le chiffrement et la signature numérique. Dans la procédure d'échange de clés, Alice et Bob produisent une clé commune (qui n'est connue que par eux), pour utiliser cette clé dans la suite. La procédure de la signature numérique permet à Bob de s'assurer que le message qu'il reçoit est bien envoyé par Alice.

— Eva veut lire le message privé d'Alice ;
— Elle peut accéder au canal public de transmission des messages ;
— Alice et Bob se mettent d'accord sur le système de chiffrement qu'ils utilisent,

et aussi sur la **clé publique** nécessaire pour chiffrer le message ;
— Bob choisit la **clé privée** pour déchiffrer le message.

Principe : tout le monde peut chiffrer (avec la clé publique), mais il n'y a que Bob qui peut déchiffrer (avec sa clé privée). Ce système est un système de chiffrement à clé asymétrique (la clé pour déchiffrer un message est différente de celle pour chiffrer).



Cette méthode a été proposée en 1976 par Whitfield Diffie et Martin Hellman : On l'appelle **la cryptographie à clé publique**.

Propriétés :
— C'est «facile» de coder le message.
— Il est très difficile de déchiffrer le message *sans connaître la clé privée* .

Signature numérique.

Principe : il n'y a qu'Alice qui peut signer (avec sa clé privée), mais tout le monde peut vérifier (avec la clé publique).

Algorithme RSA.

Proposé par Ronald Rivest, Adi Shamir et Leonard Adleman en 1978 dans l'article "A Method for Obtaining Digital Signatures and Public-key Cryptosystems".

— Les «messages» sont des nombres entiers ;
— Pour coder un message, on utilise les opérations arithmétiques : sommes, produits, divisions.

Fonctionnement de RSA :

— On choisit N un entier tel que $N = pq$ est le produit de deux (très grands) nombres premiers.
— Un «message» sera un entier m tel que $1 \leq m < N$.
— Le chiffrement : le reste r de m^e modulo N.
— Pour déchiffrer... on calcule le reste de r^f de modulo N. Comment choisit-on f ? On a

$$r \equiv m^e (\mathrm{mod}\, pq),$$

donc

$$r^f \equiv (m^e)^f = m^{ef} (\mathrm{mod}\, pq) \equiv m?$$

D'après le théorème d'Euler $m^{ef} \equiv m \pmod{\mathrm{pq}}$ si l'on prend f tel que

$$ef \equiv 1 (\mathrm{mod}\, (p-1)(q-1)).$$

Récapitulatif : Paramètres : p, q deux nombres premiers, $N = pq$, e, f tels que $ef \equiv 1 (\mathrm{mod}\, (p-1)(q-1))$.

Données publiques N, e. **Clé privée de Bob :** f.

La sécurité du système :

— On connait $r = m^e$ (modulo N), comment trouver m ?
— Pour déchiffrer il faut connaître f tel que $ef \equiv 1 (\mathrm{mod}\, (p-1)(q-1))$.
— On peut le trouver si l'on connaît p et q (problème de **factorisation**).

Ce sont des problèmes très difficiles (techniquement) ! ! !

4.2 Codes corrécteurs d'érreurs

Supposons qu'on veut transmettre un message M, mais que le canal de transmission (le radio bruité) ou le support de stockage du message (un disque rayé) peut introduire des erreurs dans les messsages. Pour qu'à la réception il soit possible d'identifier le message on transmet un message-code, qui est plus long que le message initial, et qui permet de corriger l'erreur (ou de déterminer l'existence d'une erreur) sous l'hypothèse qu'il y a au plus r erreurs.

Codes linéaires. Dans les codes linéaires on suppose que les messages sont des k-uplets $x = (x_0, \dots x_{k-1})$ d'un corps fini $\mathbb{F}_q$, pour pouvoir corriger des erreurs on représente le message par des n-uplets ($n > k$) dans $\mathbb{F}_q^n$ à l'aide d'une transformation linéaire $\mathbb{F}_q^k \to \mathbb{F}_q^n$, $x \mapsto xG$ où G est une matrice *génératrice* de k lignes et n colonnes. Le code C est dans ce cas un sous-espace linéaire de dimension k de $\mathbb{F}_q^n$. Pour determiner si le message reçu est bien un message de code, on utilise une *matrice de contrôle* : c'est une matrice H de $(n-k)$ lignes et n colonnes telle que pout tout $x \in C$ on a $H(x) = 0$. Une matrice H est une matrice de contrôle si et seulement si $H({}^tG) = 0$.

Définition 4.2.1. La *distance de Hamming* $d(x, y)$ entre deux mots x et y d'un code C est le nombre d'indices i tels que $x_i \neq y_i$. La distance minimum d de C est définie par

$$d = \min \{d(x, y), x, y \in C, x \neq y\}.$$

Pour les codes linéaires on a $d(x, y) = w(x - y)$ où $w(z)$ est le nombre de coordonnées non nulles z_i de z et on a alors $d = \min \{w(x), x \in C, x \neq 0\}$.

Proposition 4.2.2. *La distance minimum d d'un code linéaire C est le nombre minimum de colonnes de la matrice de contrôle H qui sont linéairement dépendentes.*

Définition 4.2.3. Un code linéaire pour lequel on a $d = n - k + 1$ est appelé code MDS (Maximum Distance Séparable).

Supposons qu'on a reçu un message x. Pour determiner si x est bien un message de code, on calcule $H(x)$ où H est une matrice de contrôle. Si $H(x) = 0$, c'est le cas, sinon, pour *corriger* x on lui fait correpondre le mot de code le plus proche à x au sens de la distance de Hamming, un tel mot est unique dans le cas suivant :

Proposition 4.2.4. *Si $d > 2r$ le code C corrige les r erreurs.*

Pour corriger l'erreur, on dresse alors *une table de décodage* contenant tous les éléments $e \in \mathbb{F}_q^n$ avec $w(e) \leq r$ et les valeurs $H(e)$. On décode alors x par le message $m = x - e$ où e est tel que $H(e) = H(x)$.

Les codes cycliques.

Définition 4.2.5. Un code linéaire C est *cyclique* si pour tout $m = m_0 m_1 \dots m_{n-1} \in \mathbb{F}_q^n$ dans C le mot $\sigma(m) := m_{n-1} m_0 m_1 \dots m_{n-2}$ est aussi dans C.

On reprsente chaque mot $m = m_0 m_1 \dots m_{n-1} \in \mathbb{F}_q^n$ d'un code cyclique par un polynôme

$$m(X) = m_0 + m_1 X + \ldots + m_{n-1} X^{n-1} \in \mathbb{F}_q[X].$$

Notons que

$$\sigma(m)(X) = Xm(X) + m_{n-1}(1 - X^n).$$

On peut caractériser le code cyclique de la façon suivante :

Proposition 4.2.6. *Soit C un code cyclique de longueur n et de dimension k sur $\mathbb{F}_q$. Alors :*

1. *Il exsite un unique mot $\tilde{m}$ de C tel que*

$$\tilde{m} = a_0 a_1 \dots a_{n-k-1} 10 \dots 0;$$

2. *la famille de k mots $\tilde{m}, \sigma(\tilde{m}), \dots \sigma^{k-1}(\tilde{m})$ constitue une base de C ;*
3. *le polynôme $\tilde{m}(X)$ divise le polynôme $X^n - 1$;*
4. *pour tout $m \in \mathbb{F}_q^n$ on a $m \in C \Leftrightarrow \tilde{m}(X)$ divise $m(X)$.*

Dans la situation de la proposition précédente on appelle $g = \tilde{m}(X)$ le polynôme générateur de C. Inversement, on montre que tout polynôme $g = g_0 + g_1 X + \ldots + g_{n-k-1} X^{n-k-1} + X^{n-k}$ qui divise $X^n - 1$ et le polynôme générateur d'un code cyclique C. Si $h = h_0 + \ldots + h_1 X + \ldots + h_{k-1} X^{k-1} + X^k$ est le quotient de la division euclidienne dans $\mathbb{F}_q[X]$ du polynôme $X^n - 1$ par le polynôme g, alors la matrice génératrice de C est la matrice

$$G = \begin{pmatrix} g_0 & \ldots & g_{n-k-1} & 1 & 0 & 0 & \ldots & 0 \\ 0 & g_0 & \ldots & g_{n-k-1} & 1 & 0 & \ldots & 0 \\ \ldots & & & & & & & \\ 0 & \ldots & 0 & g_0 & \ldots & g_{n-k-1} & 1 & 0 \\ 0 & 0 & \ldots & 0 & g_0 & \ldots & g_{n-k-1} & 1 \end{pmatrix}$$

et la matrice de contrôle de C est la matrice

$$H = \begin{pmatrix} 1 & h_{k-1} & \ldots & h_0 & 0 & 0 & \ldots & 0 \\ 0 & 1 & h_{k-1} & \ldots & h_0 & 0 & \ldots & 0 \\ \ldots & & & & & & & \\ 0 & \ldots & 0 & 1 & h_{k-1} & \ldots & h_0 & 0 \\ 0 & 0 & \ldots & 0 & 1 & h_{k-1} & \ldots & h_0 \end{pmatrix}$$

Les codes de Reed-Solomon. On utilise ces codes dans la lecture des DVD ou dans la transmission de donnés par satellite. Ce sont des codes cycliques sur un corps $\mathbb{F}_q$ avec $q > 2$, le plus souvent $q = 2^s$, $s > 1$, de longueur $n = q - 1$ et dimension k. Soit $\alpha \in \mathbb{F}_q^*$ un élément primitif. Rappelons que d'après (3.1) on a

$$X^{q-1} - 1 = \prod_{i=1}^{q-1}(X - \alpha^i).$$

On pose $g = \prod_{i=1}^{n-k}(X - \alpha^i)$. Le code de Reed-Solomon est un code cyclique engendré par g.

On montre que ce code est MDS, c'est-à-dire sa distance minimum vérifie $d = n - k + 1$.

Exercice. (Exemple d'un code de Reed-Solomon)
On considère le corps $\mathbb{F}_8 = \mathbb{F}_2[X]/X^3 + X + 1$ et on pose $\alpha = \bar{X}$.

1. Montrer que α est un élément primitif de $\mathbb{F}_8$: i.e. α est un générateur du groupe $\mathbb{F}_8^*$.
2. Écrire la table de logarithmes de base α : pour tout $a \in \mathbb{F}_8^*$ déterminer a tel que $a = \alpha^i$.
3. Soit $g \in \mathbb{F}_8[X]$ défini par $g = (X-\alpha)(X-\alpha^2)$. Montrer que $g = X^2+\alpha^4 X+\alpha^3$.
4. Écrire une matrice génératrice du code de Reed-Solomon C de longueur 7 engendré par g.
5. Déterminer le polynôme de contrôle et une matrice de contrôle de C.
6. En déduire que C est MDS.
7. Corriger le mot réçu $\alpha^3\alpha^2\alpha\alpha^4\alpha\alpha^4 1$.