ALGÈBRE

Najib Idrissi

M1 MIC – Université Paris Cité

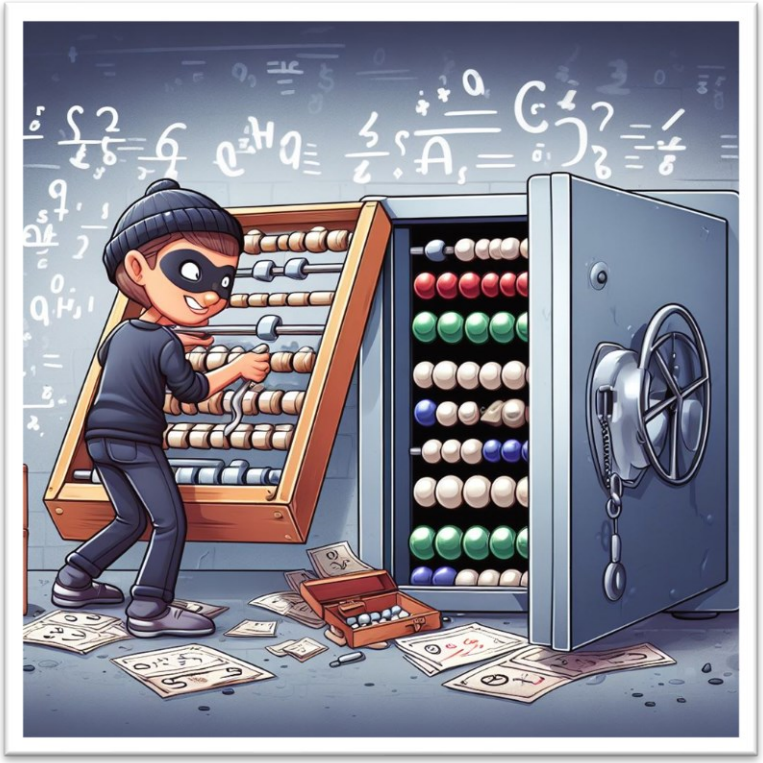


TABLE DES MATIÈRES

PRÉAMBULE

On pourra se référer à [3; 6; 8] pour des ouvrages qui traitent le contenu de ce cours (dont l'auteur de ces lignes s'est d'ailleurs largement inspiré). L'auteur remercie également Muriel Livernet pour lui avoir fourni le matériel de cours des années précédentes.

Les sections marquées par une ☆ ne sont pas au programme.

Étant donné qu'il s'agit d'un cours en master de cryptographie, nous allons donner quelques références vers des algorithmes et/ou des cas d'usage des notions présentées ici en cryptographie. L'auteur n'est pas un expert en cryptographie et ne prétend pas atteindre un quelconque degré de complétude sur le sujet. Les exemples de codes seront écrits en Mathematica (ou « langage Wolfram ») ; on pourra se référer à [12] pour une introduction rapide à ce langage.

L'image sur la page de couverture a été générée par DALL-E 2 à la suite de l'invite « *A burglar using an abacus in front of a safe covered with mathematical symbols, cartoon* ».

Notations

Commençons par quelques notations de base. On notera $\mathbb{N} = \{0, 1, \dots\}$ l'ensemble des entiers naturels et $\mathbb{Z}$ l'ensemble des entiers relatifs. En règle générale, le nom « entier » désignera un entier relatif. On note aussi $\mathbb{Q}$ l'ensemble des nombres rationnels, $\mathbb{R}$ l'ensemble des nombres réels, et $\mathbb{C}$ l'ensemble des nombres complexes. On notera enfin $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$, $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$, etc.

Soit x un nombre réel. On note $\lfloor x \rfloor$ la *partie entière* de x. C'est le plus grand entier $\leq x$. Il est caractérisé par l'inéquation $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$.

Chapitre I. ARITHMÉTIQUE DE BASE

« Six fois neuf. Quarante-deux. — C'est tout. Il n'y a rien d'autre. »

Douglas Adams, *Le Dernier Restaurant avant la fin du monde*

Section I.A. Généralités sur les groupes

Définition I.A.1. Un *groupe* consiste en la donnée d'un ensemble G, d'une fonction $G \times G \to G$, $(x, y) \mapsto x \cdot y$ (la loi de groupe) qui est associative, et d'un élément $1 \in G$ qui est une unité pour la loi de groupe, et tel que chaque élément possède un inverse. Un *morphisme de groupes* $f : G \to H$ est une fonction entre deux groupes vérifiant $f(1) = 1$ et $f(xy) = f(x)\,f(y)$ pour tous $x, y \in G$.

Étant donné $x \in G$, son inverse est unique et généralement noté x^{-1}. On se permettra souvent de ne pas écrire la loi de groupe dans les équations ($xy = x \cdot y$) sauf si cela risque de porter à confusion. Certains groupes sont notés additivement : la loi de groupe est alors notée $+$, l'unité 0, et l'inverse d'un élément x est noté $-x$.

Définition I.A.2. Un groupe est dit *commutatif* ou *abélien* si pour tous $x, y \in G$, $xy = yx$.

Exemple I.A.3. L'ensemble $\mathbb{Z}$ forme un groupe abélien pour l'addition.

Exemple I.A.4. L'ensemble des bijections $\{1, \dots, n\} \to \{1, \dots, n\}$ (où n est un entier fixé) forme un groupe pour la composition, appelé le *groupe symétrique* $\mathfrak{S}_n$. Ses éléments sont appelés les permutations de $\{1, \dots, n\}$. Ce groupe n'est pas abélien pour $n \geq 3$.

Définition I.A.5. Un *sous-groupe* H d'un groupe G est un sous-ensemble qui contient l'unité et qui est un groupe pour la loi de groupe de G restreinte à H. On notera $H \leq G$ si H est un sous-groupe de G. Étant donnés une famille $(x_1, \dots x_n, \dots)$ d'éléments de G (potentiellement infinie), on note $\langle x_1, \dots, x_n, \dots \rangle$ le plus petit sous-groupe qui contient les x_i et on l'appelle le sous-groupe engendré par la famille.

Définition I.A.6. Un sous-groupe H d'un groupe G est *distingué* (ou *normal*) s'il est stable par conjugaison, c'est-à-dire que $\forall g \in G,\ \forall h \in H,\ ghg^{-1} \in H$. On notera $H \trianglelefteq G$ si H est un sous-groupe distingué de G. Le *quotient* d'un groupe G par un sous-groupe H est noté G/H.

Remarque I.A.7. Si G est un groupe abélien, tous ses sous-groupes sont distingués.

Exemple I.A.8. Soit $f : G \to H$ un morphisme de groupes. Le noyau $\ker(f)$ forme un sous-groupe distingué de G. L'image $\mathrm{im}(f)$ forme un sous-groupe de H, qui n'est pas toujours distingué.

Proposition I.A.9. Un morphisme de groupes $f : G \to H$ induit un isomorphisme $G/\ker(f) \to \mathrm{im}(f)$.

Définition I.A.10. Soit G un groupe. Si G est fini, son cardinal est appelé *l'ordre* de G et est noté $|G|$. Étant donné $x \in G$, si le sous-groupe engendré par x, noté $\langle x \rangle$, est fini, on appelle son cardinal *l'ordre* de x. C'est le plus petit entier non-nul (s'il existe) qui vérifie $x^n = 1$.

Exemple I.A.11. Soit $n \in \mathbb{Z}$ un entier. L'ensemble $n\mathbb{Z} = \{ na \mid a \in \mathbb{Z} \}$ forme un sous-groupe de $\mathbb{Z}$. Le quotient $\mathbb{Z}/n\mathbb{Z}$ est le groupe des entiers modulo n. Il est d'ordre $|n|$ si $n \neq 0$, et il est isomorphe à $\mathbb{Z}$ si $n = 0$.

Définition I.A.12. Un groupe G est *cyclique* s'il existe un élément $g \in G$ d'ordre fini tel que $G = \langle g \rangle$.

Proposition I.A.13. Tout groupe cyclique est isomorphe à un $\mathbb{Z}/n\mathbb{Z}$ pour un certain n.

Théorème I.A.14 (Théorème de Lagrange). Soit G un groupe fini et H un sous-groupe de G. L'équation suivante est vérifiée, où $[G:H]$ est le nombre[1] de classes de G modulo l'action de H à droite :

$$|G| = |H| \times [G:H].$$

En particulier, l'ordre de H divise l'ordre de G ; et donc l'ordre d'un élément quelconque $x \in G$ divise l'ordre de G (en prenant $H = \langle x \rangle$).

Section I.B. Division euclidienne, PGCD, PPCM

Cette section ne comprend que des rappels et se passera donc de la plupart des démonstrations. Notons toutefois que plusieurs des propriétés présentées ici seront généralisées dans le Chapitre II.

§ I.B(a) Divisibilité

Théorème I.B.1. Soit a un entier quelconque et b un entier non nul. Il existe un unique couple d'entiers (q, r) vérifiant :

$$a = bq + r \text{ et } 0 \leq r < b.$$

Définition I.B.2. On appelle q le *quotient* de la division euclidienne de a par b, et r le *reste* de cette division.

Définition I.B.3. Soit m et d deux entiers. On dit que d *divise* m, ou que d est un diviseur de m,ou que m est un *multiple* de d, et on note $d \mid m$, s'il existe un entier k tel que $m = kd$.

Proposition I.B.4. Soit a, b deux entiers tels que $a \neq 0$. Alors $a \mid b$ si et seulement si le reste de la division euclidienne de b par a est nul.

Proposition I.B.5. La divisibilité définit une relation d'ordre sur $\mathbb{N}$.

Remarque I.B.6. Dans cette relation d'ordre, le plus grand élément de $\mathbb{N}$ est 0 est le plus petit est 1. En d'autres termes, quels que soit $a \in \mathbb{N}$, on a $1|a$ et $a|0$.

Remarque I.B.7. La divisibilité ne définit pas une relation d'ordre sur $\mathbb{Z}$. En effet, elle n'est pas antisymétrique :

$$(a|b \text{ et } b|a) \Leftrightarrow b = \pm a.$$

§ I.B(b) PGCD et PPCM

Définition I.B.8. Soit a et b deux entiers.

- On appelle *plus grand commun diviseur (PGCD)* de a et b le plus grand élément (pour la divisibilité) de $\mathbb{N}$ qui divise a et qui divise b, s'il existe. On le note $a \wedge b$ ou $\mathrm{pgcd}(a, b)$.
- On appelle *plus petit commun multiple (PPCM)* de a et b le plus petit élément (pour la divisibilité) de $\mathbb{N}$ qui est multiple de a et de b, s'il existe. On le note $a \vee b$ ou $\mathrm{ppcm}(a, b)$.

On définit également le PGCD et le PPCM d'une famille d'entiers $(a_1, \ldots, a_n)$ de la façon évidente.

[1] Si $H \trianglelefteq G$ est distingué alors $[G:H] = |G/H|$.

Remarque I.B.9. Le PGCD de a et b, s'il existe, est donc (l'unique) entier naturel d vérifiant les deux propriétés suivantes :

- Il divise a et b, c'est-à-dire $d|a$ et $d|b$ (c'est un « minorant » de a et b) ;
- Si c est un autre entier qui divise a et b, alors $c|d$ (parmi les minorants, c'est le plus grand).

Il s'agit donc de l'analogue la *borne inférieure* en analyse. De même, le PPCM est l'analogue de la *borne supérieure*.

Remarque I.B.10. Il est important de préciser que la relation d'ordre que l'on considère est la divisibilité et non la relation d'ordre usuelle. En effet, si l'on cherche à déterminer $0 \wedge 0$, on constate que *tous* les entiers naturels divisent 0 et 0. Il faut donc considérer le maximum de $\mathbb{N}$. Ce maximum n'existe pas pour la relation d'ordre usuelle, mais il existe pour la divisibilité et on a $0 \wedge 0 = 0$.

Proposition I.B.11. Le PGCD et le PPCM de deux entiers existent toujours.

Démonstration. Pour se convaincre de l'existence du PGCD, on peut appliquer l'algorithme d'Euclide. Si $a = b$ alors bien sûr $a \wedge b = a$. Quitte à échanger a et b, on peut donc supposer que $a > b$. On applique maintenant les étapes suivantes jusqu'à la fin de l'algorithme :

- Si $b = 0$, alors le PGCD de a et b est a.
- Sinon, on calcule le reste r de la division euclidienne de a par b.
- On remplace a par b et b par r (c.-à-d. on pose $(a, b) = (b, r)$) et on recommence.

Une fois que l'on a vérifié que cet algorithme donne bien le PGCD de a et b, on vérifie que le nombre $\frac{ab}{a \wedge b}$ est bien le PPCM de a et b. ◇

En langage Mathematica, cela donne :

```
euclide[a_, b_] /; a == b := a
euclide[a_, b_] /; a < b := euclide[b, a]
euclide[a_, 0] := a
euclide[a_, b_] := euclide[b, Mod[a, b]]
```

Exemple I.B.12. Étant donnés des entiers *naturels* $a, b, c \in \mathbb{N}$, on a les relations suivantes :

$$a \wedge a = a \vee a = a,$$

$$a \wedge 1 = 1, \qquad a \wedge 0 = a, \qquad a \vee 1 = a, \qquad a \vee 0 = 0.$$

$$a \wedge b = a \Leftrightarrow a|b \Leftrightarrow a \vee b = b,$$

$$a \wedge (a \vee b) = a = a \vee (a \wedge b),$$

$$a \wedge (b \wedge c) = (a \wedge b) \wedge c, \qquad a \vee (b \vee c) = (a \vee b) \vee c,$$

$$a \wedge (b \vee c) = (a \vee b) \wedge (a \wedge c), \qquad a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c),$$

$$ac \wedge bc = (a \wedge b)c, \qquad ac \vee bc = (a \vee b)c, \qquad (a + b) \wedge b = a \wedge b.$$

Remarque I.B.13. Ces relations font de $\mathbb{N}$ un « treillis distributif complet ».

Proposition I.B.14 (Identité de Bézout). Soit a et b deux entiers et $d = a \wedge b$ leur PGCD. Alors il existe des entiers $x, y \in \mathbb{Z}$ tels que $ax + by = d$.

Démonstration. L'algorithme d'Euclide étendu donne une preuve de ce résultat d'existence.

- On commence par poser $(r,u,v)=(a,1,0)$ et $(r',u',v')=(b,0,1)$. Dans l'algorithme qui suit, on vérifiera les invariants de boucle $r=au+bv$ et $r'=au'+bv'$.
- Tant que $r'\neq 0$, on applique les étapes suivantes :
  - On note q le quotient de la division euclidienne de r par r' et r'' le reste de cette division.
  - On pose simultanément :
$$(r,u,v,r',u',v')=(r',u',v',r'',u-qu',v-qv').$$
- L'algorithme est terminé : le PGCD d vaut r, et le couple (x,y) vaut (u,v). ◇

En code Mathematica :

```
euclideÉtendu[a_, a_] := {a, 1, 0}
euclideÉtendu[a_, b_] /; a < b := euclideÉtendu[b, a][[{1,3,2}]]
euclideÉtendu[a_, b_] := euclideÉtendu[a, 1, 0, b, 0, 1]
euclideÉtendu[r_, u_, v_, 0, _, _] := {r, u, v}
euclideÉtendu[r_, u_, v_, r2_, u2_, v2_] :=
 With[{q = Quotient[r, r2], r3 = Mod[r, r2]},
  euclideÉtendu[r2, u2, v2, r3, u - q*u2, v - q*v2]]
```

§ I.B(c) Primalité

Définition I.B.15. Deux entiers a et b sont dits *premiers entre eux* si $a\wedge b=1$.

Définition I.B.16. Soit n un entier naturel non nul. On note $\varphi(n)$ le nombre d'entiers $k\in\{1,\dots,n\}$ qui sont premiers avec n. La fonction $\varphi:\mathbb{N}^*\to\mathbb{N}^*$ s'appelle *l'indicatrice d'Euler*.

Théorème I.B.17 (Théorème de Bézout). Deux entiers a et b sont premiers entre eux si et seulement s'il existe des entiers x,y tels que $ax+by=1$.

Démonstration. L'identité de Bézout (**Proposition I.B.14**) donne l'implication directe. Pour la réciproque, suppose qu'il existe x,y tels que $ax+by=1$. Soit $d=a\wedge b$ le PGCD. Alors d divise a et d divise b, donc d divise toute combinaison linéaire entière de a et b. En particulier, d divise $ax+by=1$. Or le seul entier positif qui divise 1 est 1 lui-même, donc $d=1$. ◇

Remarque I.B.18. Bien sûr, en règle générale, s'il existe des entiers x,y tels que $ax+by=d\geq 2$, cela n'entraîne pas que $a\wedge b=d$. Par exemple, $2\times(-2)+3\times 2=2$ mais on n'a pas $2\wedge 3=2$.

Définition I.B.19. Un entier naturel p est dit *premier* s'il admet exactement deux diviseurs positifs (nécessairement 1 et lui-même). Sinon, on dit qu'il est *composé*.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96
97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112
113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128
129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144
145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176
177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192
193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208
209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224
225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240
241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256

Figure I.B-a Une table des nombres premiers inférieurs à 256.

Remarque I.B.20. L'entier 1 n'est pas premier car il n'a qu'un seul diviseur positif.

Proposition I.B.21 (Lemme d'Euclide). Soit a, b des entiers et p un nombre premier. Si p divise ab, alors p divise a ou p divise b.

Corollaire I.B.22. Soit p premier et a un entier. Soit p divise a, soit p et a sont premiers entre eux.

Corollaire I.B.23. Un entier naturel p est premier si et seulement si $\varphi(p) = p - 1$.

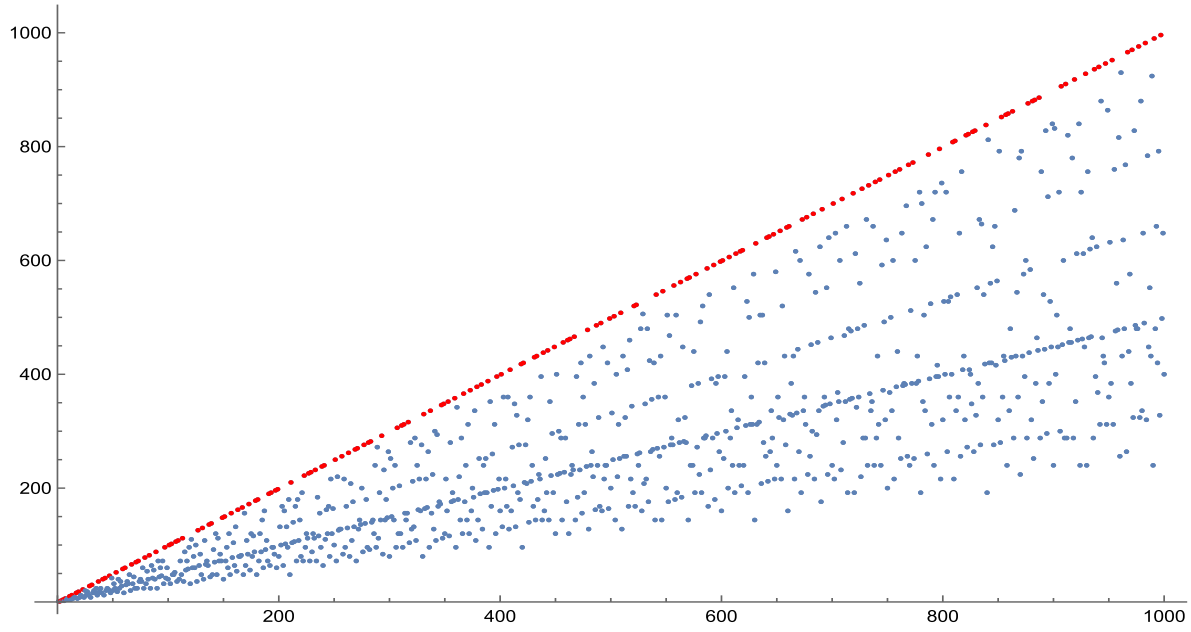


Figure I.B-b Le graphe de l'indicatrice d'Euler.
La ligne rouge représente les nombres premiers, pour lesquels $\phi(p) = p - 1$.

Proposition I.B.24 (Lemme de Gauss). Soit a, b, c des entiers quelconques. Si a divise bc et $a \wedge b = 1$ alors a divise c.

Théorème I.B.25. Soit n un entier. Il existe une famille de paires d'entiers $(p_i, \alpha_i)_{i=1}^{k}$, unique à l'ordre des facteurs près, telle que chaque p_i est premier, chaque α_i est strictement positif, et $n = \prod_{i=1}^{k} p_i^{\alpha_i}$.

Démonstration. L'existence se démontre aisément par récurrence. L'unicité découle du lemme d'Euclide. ◇

Corollaire I.B.26. Soit $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ et $m = \prod_{i=1}^{k} p_i^{\beta_i}$ deux nombres et leurs décompositions en produits de facteurs premiers (en autorisant les exposants nuls pour permettre d'avoir la même liste de nombres premiers dans les deux décompositions). Alors on a :

$$n \wedge m = \prod_{i=1}^{k} p_i^{\min(\alpha_i, \beta_i)}, \qquad n \vee m = \prod_{i=1}^{k} p_i^{\max(\alpha_i, \beta_i)}.$$

Corollaire I.B.27. Soit p un nombre premier et α un entier positif. On a $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$.

Démonstration. Il s'agit de compter les éléments $a \in \{1, \dots, p^\alpha\}$ qui sont premiers avec p^α. Comme p est premier, étant donné a, on ne peut qu'avoir $a \wedge p^\alpha = p^k$ avec $0 \leq k \leq \alpha$. Les exposants non-nuls ne surviennent que quand a est un multiple de p. Il y a $p^{\alpha-1}$ multiples de p entre 1 et p^α, à savoir les entiers $p, 2p, 3p, \dots, p^{\alpha-1}p$. Il reste en donc $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$ qui sont premiers avec le nombre p^α. ◇

Section I.C. Petit théorème de Fermat

La manière la plus « simple » de vérifier si un nombre est premier est tout simplement d'appliquer directement la définition. Étant donné un nombre $n \geq 2$, on considère tous les entiers $a \in \{2, \dots, n-1\}$ et on vérifie s'ils divisent n ou non. Si l'un d'entre eux divise p, alors n n'est pas premier ; sinon, il est premier. Mais cette méthode est peu efficace d'un point de vue algorithmique. Même en optimisant de la façon évidente, en ne considérant que les entiers $a \leq \sqrt{n}$, la complexité algorithmique en temps[2] est de l'ordre de $O\left(\sqrt{n}\ln(n)\ln(\ln(n))\right)$. Cela peut paraître faible, mais il ne faut pas oublier que la cryptographie utilise des nombres premiers de grande taille. Une clé privée RSA de 2048 bits utilise une paire de nombre premiers ayant chacun environ 1024 bits, et $2^{1000} \approx 10^{308}$. Un algorithme moderne tel qu'ECDSA-256 utilise une clé de 256 bits ($2^{256} \approx 10^{77}$). À titre de comparaison, l'univers compte environ 10^{80} atomes… Pour des nombres aussi grands, même le facteur en $\ln(\ln(n))$, qui croît très lentement et qu'on ignore habituellement, compte !

En utilisant des propriétés des nombres premiers, il est possible d'obtenir de meilleurs algorithmes. Dans cette section, nous allons voir un théorème qui permettra de mener un test de primalité plus efficace.

Théorème I.C.1. (Petit Théorème de Fermat) Soit p un nombre premier et a un entier quelconque. On a l'égalité suivante modulo p :

$$a^p \equiv a \pmod{p}.$$

[2] Le nombre de bits d'un entier n est $b = \lfloor \log_2(n) \rfloor + 1 = O(\ln(n))$. L'addition de deux nombres de taille b est de complexité $O(b) = O(\ln(n))$. La multiplication de deux nombres de taille b par la méthode « classique » est d'une complexité temporelle de l'ordre de $O(b^2) = O(\ln^2(n))$. L'algorithme de Schönhage–Strassen [10], le meilleur actuellement connu, est de complexité $O(b\ln(b)) = O(\ln(n)\ln(ln(n)))$. L'opération « modulo » qui permet de vérifier si un nombre est divisible par un autre a la même complexité temporelle que la multiplication.

Lemme I.C.2. Soit p premier et k un entier compris entre 1 et $p-1$. Le nombre p divise le coefficient binominal $\binom{p}{k}$.

Démonstration. On peut réécrire le coefficient binomial en question comme :

$$\binom{p}{k} = \frac{p(p-1)\dots(p-k+1)}{1\cdot 2\cdot \dots \cdot k}.$$

Il est clair que p divise le numérateur. De plus, p ne divise aucun des nombres du dénominateur (ils sont tous strictement inférieurs à p). Donc p divise bien la fraction. ◇

Démonstration du théorème. La preuve se fait simplement par récurrence. Le cas $a = 0$ est évident. Supposons maintenant le théorème vrai pour un entier naturel a donné. Alors :

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \dots + \binom{p}{p-1}a + 1^p.$$

D'après le lemme précédent, p divise chacun des coefficients binomiaux (hormis le premier et le dernier : $\binom{p}{p} = \binom{p}{0} = 1$). De plus, par hypothèse de récurrence, a^p et a sont congrus modulo p. On a donc l'égalité suivante modulo p :

$$\begin{aligned}(a+1)^p &\equiv a^p + 1^p \mod p \\ &\equiv a + 1 \mod p\end{aligned}$$ ◇

Remarque I.C.3. Il existe de nombreuses autres preuves de ce théorème, qui utilisent de la combinatoire, des systèmes dynamiques, les coefficients multinomiaux, la théorie des groupes…

Corollaire I.C.4. Soit p un nombre premier et a un entier qui n'est pas divisible par p. On a :

$$a^{p-1} \equiv 1 \mod p.$$

Démonstration. D'après le petit Théorème de Fermat, on a $a^p \equiv a \mod p$, c'est-à-dire que p divise $a^p - a = a(a^{p-1}-1)$. Comme a et p sont premiers entre eux, d'après le Lemme d'Euclide, on obtient que p divise $a^{p-1}-1$, ou en d'autres termes que $a^{p-1} \equiv 1 \mod p$. ◇

Le petit Théorème de Fermat donne une condition *nécessaire* pour la primalité d'un nombre entier. En effet, si p est un entier, on peut tester tous les entiers $a \in \{2, \dots, p-1\}$ et vérifier si a^p est congru à a ou pas. S'il existe un contre-exemple, alors p ne peut pas être premier. On peut ainsi parler d'un test de non-primalité. On étudiera ce test plus en détail dans la Section I.F.

Section I.D. Structure de $(\mathbb{Z}/n\mathbb{Z})^\times$

§ I.D(a) Cardinal

Définition I.D.1. On note $(\mathbb{Z}/n\mathbb{Z})^\times$ l'ensemble des éléments de $\mathbb{Z}/n\mathbb{Z}$ qui sont inversibles pour la multiplication, c'est-à-dire :

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\, a \in \mathbb{Z}/n\mathbb{Z} \mid \exists b \in \mathbb{Z}/n\mathbb{Z},\ ab = 1 \,\}.$$

Cet ensemble forme un groupe abélien pour la multiplication.

Proposition I.D.2. Soit n un entier et a un entier. Les propositions suivantes sont équivalentes :

- L'élément $[a] \in \mathbb{Z}/n\mathbb{Z}$ est inversible pour la multiplication ;
- Les nombres a et n sont premiers entre eux ;

- L'élément $[a]$ engendre le groupe abélien $(\mathbb{Z}/n\mathbb{Z}, +)$.

Démonstration. Il s'agit d'une conséquence du Théorème de Bézout (**Théorème I.B.17**). Si a est inversible, il existe b tel que $[ab] = 1$, c'est-à-dire qu'il existe $k \in \mathbb{Z}$ tel que $ab - 1 = kp$ ou encore $ab + kp = 1$. Donc a et n sont bien premiers entre eux. Réciproquement, s'ils sont premiers entre eux, alors il existe des entiers x, y tels que $ax + ny = 1$, donc $ax - 1 = -ny$ et donc $[ax] = 1$.

On note par ailleurs que si $[ax] = 1$ alors tout élément $[b] \in \mathbb{Z}/n\mathbb{Z}$ est un multiple de a car $[axb] = [b]$. Réciproquement si $[a]$ engendre le groupe additif, alors 1 est multiple de $[a]$ et donc il existe x tel que $[ax] = 1$. ◇

Corollaire I.D.3. Le cardinal de $(\mathbb{Z}/n\mathbb{Z})^\times$ est $\varphi(n)$: le nombre d'éléments de $\{1, \dots, n-1\}$ premiers avec l'entier n.

Remarque I.D.4. Ce résultat permet de donner une autre preuve du petit Théorème de Fermat. En effet, pour un nombre premier p, on a $\varphi(p) = p - 1$ (tous les éléments non-nuls de $\mathbb{Z}/p\mathbb{Z}$ sont inversibles). Or, l'ordre d'un élément d'un groupe G divise l'ordre de G (théorème de Lagrange). Appliqué au groupe $G = \mathbb{Z}/p\mathbb{Z}$, on obtient que quel que soit $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, $a^{p-1} = 1$.

Corollaire I.D.5. Si $n \geq 1$ et a sont des entiers premiers entre eux, alors :

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

Démonstration. L'ordre de $[a]$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$ divise l'ordre du groupe, qui vaut $\varphi(n)$. ◇

Corollaire I.D.6. L'anneau $\mathbb{Z}/n\mathbb{Z}$ (**Exemple II.A.10**) est un corps si et seulement si n est premier.

Démonstration. Procédons par disjonction des cas. Quitte à remplacer n par $-n$, on peut supposer que n est positif. Si $n = 0$, alors $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$ n'est pas un corps (car 2 n'est pas inversible). Si $n = 1$, alors $\mathbb{Z}/1\mathbb{Z} = 0$ n'a qu'un seul élément et n'est par définition pas un corps.

Si n est premier, alors il est premier avec tous les éléments de $\{1, \dots, n-1\}$ et toutes leurs classes dans l'anneau quotient sont donc inversibles.

Enfin, si $n \geq 2$ n'est pas premier, alors on peut écrire $n = ab$ avec $a, b \geq 2$. La classe $[a]$ n'est alors pas inversible. En effet, si elle l'était, il existerait un entier c tel que $[ac] = 1$, mais alors $[b] = [abc] = 0$ est une contradiction avec le fait que $1 < b < n$. ◇

Nous allons à présent étudier la structure du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$, qui est un groupe abélien fini (de cardinal $\varphi(n)$). Commençons par le cas le plus simple, celui où p est premier.

§ I.D(b) Cas des nombres premiers

Proposition I.D.7. Soit p un nombre premier. Le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p - 1$.

Lemme I.D.8. Pour tout entier $n \in \mathbb{N}^*$, on a (où la somme est sur les diviseurs positifs de n) :

$$n = \sum_{d|n} \varphi(d).$$

Démonstration. On partitionne $\mathbb{Z}/n\mathbb{Z}$ suivant l'ordre de ses éléments. D'après le théorème de Lagrange, l'ordre d'un élément de $\mathbb{Z}/n\mathbb{Z}$ est nécessairement un diviseur de n, donc on a :

$$\mathbb{Z}/n\mathbb{Z} = \bigsqcup_{d|n} \{\, a \in \mathbb{Z}/n\mathbb{Z} \mid a \text{ est d'ordre } d \,\}.$$

Or $\mathbb{Z}/n\mathbb{Z}$ possède un unique sous-groupe d'ordre d pour chaque diviseur d de n, à savoir $(n/d)\mathbb{Z}/n\mathbb{Z}$. Cet unique sous-groupe possède exactement $\varphi(d)$ générateurs (**Proposition I.D.2**), qui sont les éléments d'ordre d de $\mathbb{Z}/n\mathbb{Z}$. La partition ci-dessus donne donc $n = \sum_{d|n} \varphi(d)$ comme voulu. ◇

Lemme I.D.9. Soit $\mathbb{K}$ un corps fini. Le groupe $\mathbb{K}^\times$ est cyclique.

Démonstration. Soit $n = |\mathbb{K}^\times|$. Étant donné un diviseur d de n, on note ν_d le nombre d'éléments de $\mathbb{K}^\times$ d'ordre d.

Supposons qu'il existe $x \in \mathbb{K}^\times$ d'ordre d pour un certain d. Alors le sous-groupe $\langle x \rangle \subset \mathbb{K}^\times$ engendré par x contient d éléments, et quel que soit $y = x^k \in \langle x \rangle$, on a $y^d = (x^k)^d = x^{kd} = 1$. Les éléments de $\langle x \rangle$ sont donc des racines du polynôme $X^d - 1 \in \mathbb{K}[X]$. Or, un polynôme de degré d dans un corps ne peut avoir au plus que d racines.[3] Donc $\langle x \rangle$ contient exactement les racines de $X^d - 1$, c'est-à-dire que tous les éléments d'ordre d sont dans $\langle x \rangle$. Comme $\langle x \rangle$ est un groupe cyclique, il contient $\varphi(d)$ éléments d'ordre d.

Il en résulte que soit $\nu_d = \varphi(d)$ (si un tel x existe), soit $\nu_d = 0$ (si x n'existe pas). Or, tout élément de $\mathbb{K}^\times$ a un ordre d qui divise n, donc on a la double égalité :

$$\sum_{d|n} \nu_d = n = \sum_{d|n} \varphi(d).$$

On en déduit donc que $\nu_d = \varphi(d)$ pour tout d (sinon, la somme de gauche serait strictement inférieure à celle de droite). En particulier, $\nu_n = \varphi(n) > 0$ et donc $\mathbb{K}^\times$ contient au moins un élément d'ordre n. Comme n est le cardinal de $\mathbb{K}^\times$, c'est que ce groupe est cyclique. ◇

Remarque I.D.10. La même preuve permet de démontrer que si $\mathbb{K}$ est un corps quelconque (potentiellement infini) et si $G \leq \mathbb{K}^\times$ est un sous-groupe fini, alors G est cyclique.

Démonstration de la proposition. L'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps, donc son groupe des unités est cyclique. Son ordre est bien $\varphi(p) = p - 1$ grâce à la **Proposition I.D.2**. ◇

Remarque I.D.11. Déterminer un générateur du groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ (appelés les racines primitives modulo p) est un problème difficile ! De plus, étant donné une racine primitive r modulo p et un élément $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, il n'y a pas de méthode efficace en général pour trouver l'exposant k tel que $r^k = a$, appelé « logarithme discret » de a (en base r, modulo p). Cette difficulté est à la base de plusieurs algorithmes cryptographiques, comme l'échange de clés de Diffie–Hellman.

§ I.D(c) Cas des puissances d'un nombre premier impair

Proposition I.D.12. Soit p un nombre premier impair et $\alpha \geq 2$ un entier. Alors $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est un groupe cyclique d'ordre $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$.

Remarque I.D.13. Comme $\mathbb{Z}/p^\alpha\mathbb{Z}$ n'est pas un corps, le fait que son groupe des unités est cyclique n'a rien d'automatique !

[3] Pour s'en convaincre, démontrer ce résultat par récurrence sur d et la division euclidienne : si α est une racine de $P \in \mathbb{K}[X]$, alors $P = (X - \alpha)Q + c$ pour $Q \in \mathbb{K}[X]$ et $c \in \mathbb{K}$; en évaluant en α, on a $c = 0$. Cependant, l'utilisation de la division euclidienne des polynômes nécessite quelques notions sur les anneaux qui seront démontrées dans le Chapitre II. On vérifiera qu'il n'y a pas de boucle logique !

Comme on sait que $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$, il suffit de trouver un élément de cet ordre pour conclure. Nous allons exprimer cet élément comme un produit de deux éléments, l'un d'ordre $p^{\alpha-1}$ et l'autre d'ordre $p-1$, et utiliser le lemme suivant :

Lemme I.D.14. Soit G un groupe et deux éléments $a, b \in G$ qui commutent et d'ordres respectifs k, l premiers entre eux. Alors ab est d'ordre kl.

Démonstration. Notons n l'ordre de ab. D'une part, comme a et b commutent, on a $(ab)^{kl} = a^{kl}b^{kl} = 1$ donc n divise kl. D'autre part, on a $(ab)^n = 1$, donc en élevant à la puissance l, on a $a^{nl} = a^{nl}b^{nl} = (ab)^{nl} = 1$. L'ordre k de a divise donc nl. Or, k et l sont premiers entre eux, donc k divise n. Symétriquement, on trouve que l divise n. Leur PPCM, qui n'est autre que $k \vee l = kl$, divise donc n. Ces deux relations de divisibilité entraînent que $n = kl$. ◇

Remarque I.D.15. L'hypothèse que a et b commutent est essentielle (considérer les cycles $(1\ 2)$ et $(1\ 2\ 3)$ dans le groupe symétrique). Si k et l ne sont pas premiers entre eux, on ne peut pas remplacer kl par le PPCM dans l'énoncé (penser au produit aa^{-1}).

Lemme I.D.16. Soit $k \in \mathbb{N}$ un entier naturel. Il existe un entier λ_k premier à p tel que :

$$(1+p)^{p^k} = 1 + \lambda_k p^{k+1}.$$

Remarque I.D.17. L'analogue de ce lemme est faux pour $p = 2$: si $k \neq 0$, l'entier $\left(3^{2^k} - 1\right)/2^{k+1}$ est pair. Nous verrons ci-dessous comment résoudre ce problème.

Démonstration. Démontrons ceci par récurrence. Le cas $k = 0$ est évident : il suffit de choisir $\lambda = 1$. Supposons maintenant que l'équation est vérifiée pour un rang k donné. On a alors :

$$\begin{aligned}(1+p)^{p^{k+1}} &= (1+\lambda_k p^{k+1})^p = \sum_{i=0}^{p} \binom{p}{i} (\lambda_k)^i p^{(k+1)i} \\ &= 1 + \lambda_k p^{k+2} + p^{k+3} \sum_{i=2}^{p-1} \binom{p}{i} (\lambda_k)^i p^{(k+1)i-k-3} + (\lambda_k)^p p^{(k+1)p} \\ &= 1 + (\lambda_k + up) p^{k+2}.\end{aligned}$$

On remarquera que l'on a utilisé l'hypothèse $p \geq 3$ pour la dernière factorisation. Dans le dernier terme, $\lambda_{k+1} \coloneqq \lambda_k + up$ est bien premier avec p. ◇

Corollaire I.D.18. L'élément $[1+p] \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est d'ordre $p^{\alpha-1}$.

Démonstration. Tout d'abord, on a que :

$$(1+p)^{p^{\alpha-1}} = 1 + \lambda_{\alpha-1} p^\alpha \equiv 1 \bmod p^\alpha.$$

Donc l'ordre de $1+p$ divise $p^{\alpha-1}$. De plus, $(1+p)^{p^{\alpha-2}} = 1 + \lambda_{\alpha-2} p^{\alpha-1}$. Comme p ne divise pas $\lambda_{\alpha-2}$, on a que p^α ne divise pas le produit $\lambda_{\alpha-2} p^{\alpha-1}$, donc $1 + \lambda_{\alpha-2} p^{\alpha-1} \not\equiv 1 \bmod p^\alpha$ et l'ordre de $1+p$ est bien égal à $p^{\alpha-1}$. ◇

Lemme I.D.19. Le groupe $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ contient un élément d'ordre $p-1$.

Démonstration. Considérons le morphisme d'anneau $\psi\colon \mathbb{Z}/p^\alpha\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ donné par l'identité de $\mathbb{Z}$. Il induit un morphisme de groupes $\psi\colon (\mathbb{Z}/p^\alpha\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$. Ce morphisme est surjectif : étant donné une classe $[a] \in (\mathbb{Z}/p\mathbb{Z})^\times$, l'entier $a \in \mathbb{Z}$ est premier avec p et est donc premier avec p^α, et on a bien $[a] \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ et $\psi([a]) = [a]$. Or on a vu que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p-1$. Choisissons un

générateur $g' \in (\mathbb{Z}/p\mathbb{Z})^\times$, que l'on relève en $g \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. Comme g' est d'ordre $p-1$, g est d'ordre un multiple de $p-1$ et donc $\langle g \rangle$ contient un élément d'ordre $p-1$. ◇

Démonstration de la proposition. Nous venons de voir que $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ contient un élément g d'ordre $p-1$ et un élément $1+p$ d'ordre $p^{\alpha-1}$. Comme ces deux ordres sont premiers entre eux et que $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est abélien, le produit $(1+p)g$ est d'ordre $p^{\alpha-1}(p-1) = \varphi(p^\alpha)$. ◇

§ I.D(d) Cas des puissances de 2

Proposition I.D.20. Soit $\alpha \geq 1$ un entier. Le groupe $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ est donné par :

- Si $\alpha = 1$, alors $(\mathbb{Z}/2\mathbb{Z})^\times = 1$ est le groupe trivial.
- Si $\alpha = 2$, alors $(\mathbb{Z}/4\mathbb{Z})^\times = \{1,3\} \cong \mathbb{Z}/2\mathbb{Z}$ est le groupe (cyclique) à deux éléments.
- Si $\alpha \geq 3$, alors $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$.

Lemme I.D.21. Soit $k \in \mathbb{N}$ un entier naturel, il existe un nombre impair μ_k tel que :

$$5^{2^k} = 1 + \mu_k 2^{k+2}.$$

Démonstration. Le cas $k = 0$ est clair ($5^1 = 1 + 1 \times 4$ donc on peut prendre $\mu_0 = 1$). Supposons l'égalité vraie pour un rang k donné. Alors :

$$5^{2^{k+1}} = (1 + \mu_k 2^{k+2})^2 = 1 + \mu_k 2^{k+3} + \mu_k^2 2^{2k+4} = 1 + (\mu_k + 2\mu_k^2)2^{k+3}.$$

Il suffit donc de poser $\mu_{k+1} = \mu_k + 2\mu_k^2$ qui est impair. ◇

Démonstration de la proposition. Les deux premiers cas sont évidents. Posons donc $\alpha \geq 3$. Soit $\psi\colon \mathbb{Z}/2^\alpha\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ la réduction mod 4, qui induit un morphisme de groupes $\psi\colon (\mathbb{Z}/2^\alpha\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times$. Ce morphisme est surjectif, car $\psi(1) = 3$ et $\psi(3) = 3$. Donc $\ker(\psi)$ est d'ordre :

$$|\ker(\psi)| = \frac{|(\mathbb{Z}/2^\alpha\mathbb{Z})^\times|}{|(\mathbb{Z}/4\mathbb{Z})^\times|} = \frac{\phi(2^\alpha)}{\phi(4)} = \frac{2^{\alpha-1}}{2} = 2^{\alpha-2}.$$

Or, $\ker(\psi)$ contient 5 (car $5 \equiv 1 \bmod 4$) et le lemme précédent démontre que 5 est d'ordre $2^{\alpha-2}$, donc $\ker(\psi)$ est cyclique. Il nous suffit donc de démontrer que $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ est isomorphe au produit de $\ker(\psi)$ et de $(\mathbb{Z}/4\mathbb{Z})^\times$. C'est une conséquence du lemme suivant, appliqué à $\sigma(\pm 1) = \pm 1$. ◇

Lemme I.D.22. Soit $\psi\colon G \to H$ un morphisme surjectif de groupes abéliens. S'il existe un morphisme $\sigma\colon H \to G$ tel que $\psi \circ \sigma = \mathrm{id}_H$, alors G est isomorphe à $H \times \ker(\psi)$.

On définit un morphisme de groupes $\rho\colon G \to \ker(\psi)$ par $\rho(g) = g - \sigma\big(\psi(g)\big)$ (qui est bien un morphisme car G est abélien). Cela nous permet ainsi de définir un morphisme de groupes $(\psi, \rho)\colon G \to H \times \ker(\psi)$.

Comme G et $H \times \ker(\psi)$ ont le même cardinal, il suffit de démontrer que le morphisme (ψ, ρ) est injectif pour en déduire que c'est un isomorphisme. Supposons donc que $g \in G$ est dans le noyau de (ψ, ρ), c'est-à-dire que $\psi(g) = 0$ et $\rho(g) = 0$. En particulier, $\rho(g) = g - \sigma\big(\psi(g)\big) = g - \sigma(0) = g$, d'où l'on en déduit que $g = 0$. ◇

§ I.D(e) Cas général

Théorème I.D.23. Soit $n = \prod_{i=1}^k p_i^{\alpha_i}$ un entier naturel et sa décomposition en facteur premiers distincts. On a un isomorphisme de groupes :

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_{i=1}^{k} \left(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}\right)^\times.$$

Ainsi qu'une égalité :

$$\varphi(n) = \prod_{i=1}^{k} \varphi\left(p_i^{\alpha_i}\right) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Étant donné les résultats des sections précédentes, le théorème découle directement du résultat suivant et d'une récurrence :

Théorème I.D.24 (Théorème des restes chinois). Soit a et b deux entiers premiers entre eux. Il y a un isomorphisme d'anneaux :

$$\mathbb{Z}/ab\mathbb{Z} \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}.$$

Démonstration. Il y a un morphisme de groupes évident $\mathbb{Z}/ab\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ donné par $[n] \mapsto ([n], [n])$. Il suffit de montrer qu'il est injectif, car les deux groupes ont bien entendu le même cardinal. Si $[n]$ appartient au noyau, c'est que a et b divisent n ; leur PPCM $a \vee b = ab$ (ils sont premiers entre eux) divise donc également n, donc $[n] = 0 \in \mathbb{Z}/ab\mathbb{Z}$. ◇

Remarque I.D.25. Ce résultat est évidemment faux si a et b ne sont pas premiers entre eux. Par exemple, $\mathbb{Z}/4\mathbb{Z}$ n'est pas isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Corollaire I.D.26. L'indicatrice d'Euler est multiplicative : si a et b sont des nombres premiers entre eux, alors $\varphi(ab) = \varphi(a)\,\varphi(b)$.

Remarque I.D.27. Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si et seulement si n vaut 2 ou 4 ou est de la forme p^α ou $2p^\alpha$ avec p un nombre premier impair.

Remarque I.D.28. Le théorème des restes chinois (appliqué plusieurs fois) dit qu'étant donnés des entiers $n_1, \dots, n_k$ premiers entre eux deux à deux et des classes $a_1 \in \mathbb{Z}/n_1\mathbb{Z}, \dots, a_k \in \mathbb{Z}/n_k\mathbb{Z}$, si on note $N = n_1 \dots n_k$, alors il existe une unique classe $x \in \mathbb{Z}/N\mathbb{Z}$ telle que $x \equiv a_i \pmod{n_i}$ pour tout $1 \leq i \leq k$.

La preuve donnée ci-dessus n'est pas constructive, mais on peut en fait facilement trouver la solution. Soit $m_i = N/n_i = n_1 \dots \hat{n_i} \dots n_k$. Comme n_i et m_i sont premiers entre eux, il existe un entier λ_i tel que $m_i\lambda_i \equiv 1 \pmod{n_i}$. Une solution au système d'équations modulaires est alors donnée par :

$$x \coloneqq \lambda_1 m_1 a_1 + \cdots \lambda_k m_k a_k.$$

En code :

```
restesChinois[a_, n_] /; Length[a] == Length[n] :=
 Module[{prod, m, λ},
  prod = Times @@ n;
  m = prod/n;
  λ = MapThread[euclideÉtendu[#, #2][[2]] &, {m, n}];
  Mod[Plus @@ (λ*m*a), grandN]
  ]
```

Section I.E. Réciprocité quadratique

Pour cette section, on pourra se référer notamment à [5].

§ I.E(a) Symbole de Legendre

Définition I.E.1. Soit p un nombre premier et a un entier. On dit que a est un *résidu quadratique* mod p s'il existe un entier n tel que $a \equiv n^2 \bmod p$.

Exemple I.E.2. Si a est déjà un carré dans $\mathbb{Z}$, alors c'est un résidu quadratique quel que soit p.

Exemple I.E.3. Le nombre 3 est un résidu quadratique modulo 11, car $5^2 = 25 = 3 + 2 \times 22$. Ce n'est en revanche pas un résidu quadratique modulo 5 ou 7.

Définition I.E.4. Soit $p \geq 3$ un nombre premier et a un entier. On définit le *symbole de Legendre*, noté $\left(\frac{a}{p}\right)$, de la façon suivante :

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{si } a \text{ est un résidu quadratique mod } p \text{ et } a \not\equiv 0 \bmod p\,; \\ -1, & \text{si } a \text{ n'est pas un résidu quadratique mod } p; \\ 0, & \text{si } a \equiv 0 \bmod p\,. \end{cases}$$

Avertissement I.E.5. Il ne faudra pas confondre cette notation avec celle d'une fraction…

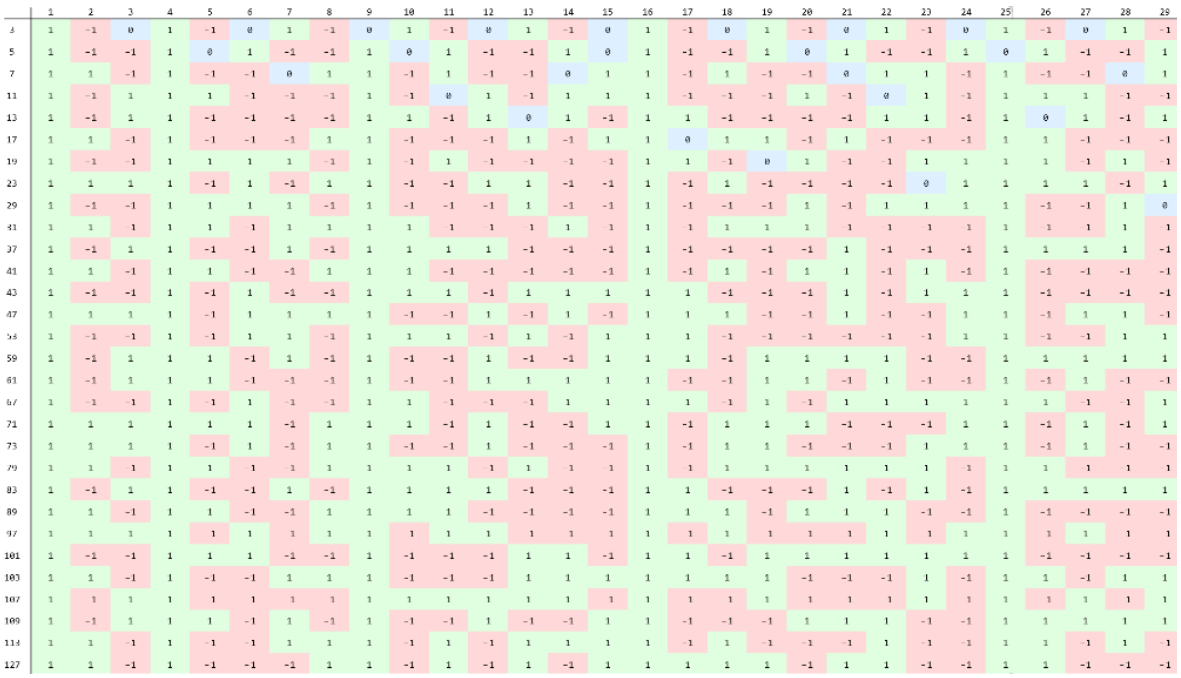


Figure I.E-a Les premières valeurs du symbole de Legendre $\left(\frac{a}{p}\right)$ (a en abscisse, p en ordonnée).

Remarque I.E.6. Le symbole de Legendre $\left(\frac{a}{p}\right)$ ne dépend que de la classe de $a \bmod p$.

Proposition I.E.7. Le symbole de Legendre est complètement multiplicatif en la première variable : pour tout premier $p \geq 3$, on a $\left(\frac{1}{p}\right) = 1$, et pour tous $a, b \in \mathbb{Z}$ on $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Démonstration. La démonstration est un petit exercice de disjonction des cas. ◇

Proposition I.E.8 (Critère d'Euler). Soit $p \geq 3$ un nombre premier et a un entier. On a :

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p.$$

Démonstration. Le cas où a est divisible par p est clair, supposons donc que $a \wedge p = 1$. D'après le petit Théorème de Fermat, on a $[a^{p-1}] = 1$, ce que l'on peut réécrire en :

$$\left[a^{\frac{p-1}{2}} - 1\right]\left[a^{\frac{p-1}{2}} + 1\right] = 0. \qquad (*)$$

D'après le Lemme d'Euler, au moins une des deux congruences $\left[a^{\frac{p-1}{2}}\right] = 1$ ou $\left[a^{\frac{p-1}{2}}\right] = -1$ est vraie. De plus, si a est un résidu quadratique (et donc $\left(\frac{a}{p}\right) = 1$), disons $[a] = [x^2]$, alors :

$$\left[a^{\frac{p-1}{2}}\right] = \left[(x^2)^{\frac{p-1}{2}}\right] = [x^{p-1}] = 1.$$

Donc la congruence $\left[\left(\frac{a}{p}\right)\right] = \left[a^{\frac{p-1}{2}}\right]$ est vérifiée. Il nous reste donc à montrer que si a n'est pas un résidu quadratique, alors $\left[a^{\frac{p-1}{2}}\right] = -1$. Or, le polynôme $X^{\frac{p-1}{2}} - 1 \in (\mathbb{Z}/p\mathbb{Z})[X]$ ne peut avoir au plus que $\frac{p-1}{2}$ racines, car $\mathbb{Z}/p\mathbb{Z}$ est un corps. Il suffit donc de démontrer qu'il y a au moins $\frac{p-1}{2}$ résidus quadratiques non-nuls pour conclure : si a n'est pas un résidu quadratique, alors il ne peut pas être racine de $X^{\frac{p-1}{2}} - 1$ et donc d'après $(*)$ on doit avoir $\left[a^{\frac{p-1}{2}}\right] = -1$.

L'application $\sigma: (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\} \to (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$, $x \mapsto x^2$ a pour image l'ensemble des résidus quadratiques non-nuls. De plus, pour un $a \neq 0$ donné, la préimage $\sigma^{-1}(\{a\})$ est l'ensemble des racines du polynôme $X^2 - a$. Son cardinal est donc au plus égal à 2, toujours car $\mathbb{Z}/p\mathbb{Z}$ est un corps. Si l'on note R le nombre de résidus quadratiques non-nuls, on obtient donc que le cardinal de $(\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$, qui vaut bien sûr $p - 1$, est inférieur ou égal à $2R$ et donc que $R \geq \frac{p-1}{2}$. Il y a donc bien au moins $\frac{p-1}{2}$ résidus quadratiques non-nuls. ◇

Notons que nous avons démontré au passage :

Proposition I.E.9. Soit p un nombre premier. Il y a autant d'éléments de $(\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$ qui sont des résidus quadratiques que d'éléments qui n'en sont pas.

Remarque I.E.10. L'application $x \mapsto p - x$ est une involution libre (car $p \neq 2$) sur l'ensemble $(\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$. Si $a = x^2$ est un résidu quadratique non-nul, alors $(p - x)^2 = a$ est l'autre manière de voir a comme un résidu quadratique. Par exemple, $x^2 \equiv 19 \mod 31$ admet la solution $x = 9$, donc l'autre solution est $31 - x = 22$.

§ I.E(b) Loi de réciprocité quadratique

Terminons ce chapitre sur le résultat fondamental suivant. Ce résultat relie deux énoncés qui n'ont, a priori, aucun rapport entre eux : le fait qu'un nombre premier soit ou pas un résidu quadratique modulo un autre nombre premier q, et la réciproque, à savoir que q est ou pas un résidu quadratique modulo p.

Théorème I.E.11 (Réciprocité quadratique). Soit p et q deux nombres premiers impairs distincts. Alors l'équation suivante est vérifiée :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}.$$

En d'autres termes :

- Si au moins l'un des deux nombres p et q est congru à 1 modulo 4, alors p est un résidu quadratique modulo q si et seulement si q est un résidu quadratique modulo p.
- Sinon (si les deux nombres p et q sont congrus à 3 modulo 4), alors p est un résidu quadratique modulo q si et seulement si q **n'est pas** un résidu quadratique modulo p.

Remarque I.E.12. En théorie des nombres, il est fréquent de noter

$$p^* \coloneqq \left(\frac{-1}{p}\right) p = (-1)^{\frac{p-1}{2}} p.$$

La réciprocité quadratique peut se réécrire comme $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$.

	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73
3	0	-1	1	-1	1	-1	1	-1	-1	1	1	-1	1	-1	-1	-1	1	1	-1	1
5	-1	0	-1	1	-1	-1	1	-1	1	1	-1	1	-1	-1	-1	1	1	-1	1	-1
7	-1	-1	0	1	-1	-1	-1	1	1	-1	1	-1	1	-1	1	-1	-1	1	1	-1
11	1	1	-1	0	-1	-1	-1	1	-1	1	1	-1	-1	1	1	1	-1	1	1	-1
13	1	-1	-1	-1	0	1	-1	1	1	-1	-1	-1	1	-1	1	-1	1	-1	-1	-1
17	-1	-1	-1	-1	1	0	1	-1	-1	-1	-1	-1	1	1	1	1	-1	1	-1	-1
19	-1	1	1	1	-1	1	0	1	-1	-1	-1	-1	1	1	-1	-1	1	-1	-1	1
23	1	-1	-1	-1	1	-1	-1	0	1	1	-1	1	-1	1	-1	1	-1	-1	1	1
29	-1	1	1	-1	1	-1	-1	1	0	-1	-1	-1	-1	-1	1	1	-1	1	1	-1
31	-1	1	1	-1	-1	-1	1	-1	-1	0	-1	1	-1	1	-1	1	-1	1	1	-1
37	1	-1	1	1	-1	-1	-1	-1	-1	-1	0	1	-1	1	1	-1	-1	1	1	1
41	-1	1	-1	-1	-1	-1	-1	1	-1	1	1	0	1	-1	-1	1	1	-1	-1	1
43	-1	-1	-1	1	1	1	-1	1	-1	1	-1	1	0	1	1	1	-1	1	-1	-1
47	1	-1	1	-1	-1	1	-1	-1	-1	-1	1	-1	-1	0	1	1	1	-1	1	-1
53	-1	-1	1	1	1	1	-1	-1	1	-1	1	-1	1	1	0	1	-1	-1	-1	-1
59	1	1	1	-1	-1	1	1	-1	1	-1	-1	1	-1	-1	1	0	-1	-1	1	-1
61	1	1	-1	-1	1	-1	1	-1	-1	-1	-1	1	-1	1	-1	-1	0	-1	-1	1
67	-1	-1	-1	-1	-1	1	1	1	1	-1	1	-1	-1	1	-1	1	-1	0	1	1
71	1	1	-1	-1	-1	-1	1	-1	1	-1	1	-1	1	-1	-1	-1	-1	-1	0	1
73	1	-1	-1	-1	-1	-1	1	1	-1	-1	1	1	-1	-1	-1	-1	1	1	1	0

Figure I.E-b Valeurs de $\left(\frac{p}{q}\right)$ pour des petits nombres premiers. En rouge et vert, les entrées symétriques ; en bleu et violet, les entrées antisymétriques.

Ce théorème est complété par deux autres lois de « réciprocité » :

Théorème I.E.13 (Premier complément). Soit p un nombre premier impair. Le nombre -1 est un résidu quadratique modulo p si et seulement si p est congru à 1 modulo 4, c'est-à-dire :

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Démonstration. Nous pouvons déjà démontrer le premier complément, qui est une conséquence immédiate du critère d'Euler (**Proposition I.E.8**). En effet, ce critère donne $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \ [p]$. Or, il s'agit de deux nombres égaux à ± 1, et $p \geq 3$. Ils sont donc égaux. ◇

Remarque I.E.14. Comme $\left(\frac{p}{-1}\right) = 1$ quel que soit p et que $(-1)^{\frac{(p-1)}{2}\left(\frac{-1-1}{2}\right)} = (-1)^{\frac{p-1}{2}}$, ce premier complément est bien une variante de la réciprocité quadratique.

Théorème I.E.15 (Deuxième complément). Soit p un nombre premier impair. Le nombre 2 est un résidu quadratique modulo p si et seulement si p est congru à 1 ou -1 modulo 8, c'est-à-dire :

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Avant de démontrer le résultat, donnons quelques exemples d'application.

Exemple I.E.16. Est-ce que $x^2 \equiv 5 \ [103]$ a une solution ? Difficile de répondre à première vue, à part en testant tous les entiers $x \in \{0, \dots, 102\}$. Mais comme 5 est congru à 1 modulo 4, on a $\left(\frac{5}{103}\right) = \left(\frac{103}{5}\right)$. Or, $103 \equiv 3 \ [5]$ n'est pas un résidu quadratique, donc 103 n'est pas un résidu quadratique mod 5.

Exemple I.E.17. Comment calculer $\left(\frac{79}{101}\right)$? Comme $101 \equiv 1 \ [4]$, on a :

$$\left(\frac{79}{101}\right) = \left(\frac{101}{79}\right) = \left(\frac{22}{79}\right) = \left(\frac{2}{79}\right)\left(\frac{11}{79}\right).$$

D'après le second complément, $\left(\frac{2}{79}\right) = 1$. De plus, 11 et 79 sont congrus à 3 mod 4 donc :

$$\left(\frac{11}{79}\right) = -\left(\frac{79}{11}\right) = -\left(\frac{2}{11}\right) = 1.$$

L'équation $x^2 = 79$ admet donc bien une solution modulo 101. Un calcul numérique laborieux permet de trouver les solutions $x = 33$ et $x = 101 - 33 = 68$.

Remarque I.E.18. Malheureusement, le théorème de réciprocité quadratique n'est pas *constructif*. Il permet de déterminer si l'équation $x^2 \equiv p \bmod q$ a une solution ou non, mais ne donne pas la solution si elle existe.

Exemple I.E.19. Soit p un nombre premier impair. Alors l'équation $x^2 \equiv -1 \bmod p$ admet une solution si et seulement si p est congru à 1 modulo 4, car si $p = 4k + r$ alors

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{r-1}{2}} = \begin{cases} 1, & \text{si } r = 1 ; \\ -1, & \text{si } r = 3. \end{cases}$$

Donc -1 est un carré modulo $5, 13, 17, 29$, etc., mais pas modulo $3, 7, 11, 19$, etc.

Corollaire I.E.20. Il existe une infinité de nombres premiers p congrus à 1 modulo 4.

Démonstration. Supposons au contraire qu'il en existe un nombre fini, disons $\{p_1, \dots p_k\}$. Considérons l'entier :

$$a = (2p_1 \dots p_k)^2 + 1.$$

Soit q un facteur premier de a. Alors l'équation $x^2 = -1$ a une solution modulo q, à savoir $x = 2p_1 \dots p_m$. D'après la loi de réciprocité quadratique, $p \equiv 1 \bmod 4$. Or, a est premier avec tous les p_i, donc q aussi. C'est donc un nouveau nombre premier congru à 1 modulo 4. ◇

Corollaire I.E.21. Il existe une infinité de nombres premiers congrus à -1 modulo 8.

Démonstration. L'idée est la même que dans le corollaire précédent. Soit $\{p_1, \dots, p_k\}$ un ensemble de nombre premiers congrus à -1 mod 8. On pose :

$$a = (4p_1 \dots p_k)^2 - 2.$$

Étant donné un facteur premier impair q de a, l'équation $x^2 \equiv 2\ [q]$ a une solution, donc $q \equiv \pm 1 \bmod 8$. Or, $a \equiv -2 \bmod 8$, donc au moins l'un de ses facteurs premiers impairs est congru à -1. Ce facteur est premier avec tous les p_i et donne donc un nombre premier congru à $-1 \bmod 8$ qui ne figure pas dans la liste $\{p_1, \dots, p_k\}$. ◇

(i) Une preuve combinatoire

Il existe de nombreuses preuves de la réciprocité quadratique. Donnons-en une, purement combinatoire, due à Eisenstein (voir par exemple [7, §3.2]).

Théorème I.E.22 (Lemme de Gauss[4]). Soit p un nombre premier impair et a un entier non divisible par p. Soit S l'ensemble des restes de la division euclidienne par p des nombres $\left\{a, 2a, 3a, \dots, \frac{p-1}{2}a\right\}$ et soit n le nombre d'éléments de S qui sont supérieurs à $p/2$. Alors :

$$\left(\frac{a}{p}\right) = (-1)^n.$$

Exemple I.E.23. Soit $p = 13$ et $a = 6$. On doit considérer les nombres $\{6, 12, 18, 24, 30, 36\}$, dont les restes mod 13 sont $\{6, 12, 5, 11, 4, 10\}$. Parmi ces restes, trois sont supérieurs à $13/2$, donc le théorème prédit $\left(\frac{6}{13}\right) = -1$, c'est-à-dire que 6 n'est pas un résidu mod 13. On peut vérifier que c'est effectivement le cas (les classes des résidus non-nuls mod 13 sont $\{1, 3, 4, 9, 10, 12\}$).

Démonstration du Lemme de Gauss. On pose le produit suivant :

$$X = \prod S = \prod_{k=1}^{n} ka = a \times 2a \times 3a \times \dots \times \frac{p-1}{2}a.$$

Ce produit peut être simplifié en :

$$X = a^{\frac{p-1}{2}} 1 \times 2 \times \dots \times \frac{p-1}{2} = a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!$$

Nous allons maintenant calculer ce produit (modulo p) d'une autre manière. Soient $x_1, \dots, x_n$ les restes supérieurs à $p/2$ et $y_1, \dots, y_m$ les restes inférieurs à $p/2$. Aucun n'est nul (car aucun élément de S n'est divisible par p) et on a $n + m = \frac{p-1}{2}$. Par définition, $X = x_1 \dots x_n y_1 \dots y_m$.

Pour tout i, on a $0 < p - x_i < \frac{p-1}{2}$ et les valeurs $p - x_i$ sont deux à deux distinctes. De plus, aucun $p - x_i$ n'est égal à un y_j (car sinon, on aurait $p - ka \equiv la \bmod p$) pour deux valeurs distinctes $1 \leq k, l \leq \frac{p-1}{2}$ et donc $k + l \equiv 0\ [p]$, ce qui est impossible). Posons :

$$E = \{p - x_1, \dots, p - x_n\} \cup \{y_1, \dots, y_m\}.$$

Cet ensemble contient $\frac{p-1}{2}$ valeurs distinctes deux à deux entre 1 et $\frac{p-1}{2}$. C'est donc que E est exactement l'ensemble $\left\{1, \dots, \frac{p-1}{2}\right\}$. Donc :

$$(p - x_1) \dots (p - x_n) y_1 \dots y_m = \left(\frac{p-1}{2}\right)!$$

[4] Gauss a démontré de nombreux lemmes…

Or, modulo p, ce produit est congru à $(-1)^n X$. Comme $\left(\frac{p-1}{2}\right)!$ est inversible modulo p, on en déduit que $a^{\frac{p-1}{2}} \equiv (-1)^n \ [p]$. Il ne reste plus qu'à appliquer le critère d'Euler (**Proposition I.E.8**) pour conclure. ◇

Théorème I.E.24 (Lemme d'Eisenstein). Soit p un premier impair.

- Si a un nombre impair non divisible par p, on a :
$$\left(\frac{a}{p}\right) = (-1)^{t_a}, \text{ où } t_a = \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{ka}{p} \right\rfloor.$$
- Si $a = 2$, on a :
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Démonstration. Utilisons les mêmes notations que dans la preuve du théorème précédent. Il suffit de montrer que $n \equiv t \quad [2]$ pour le premier cas, ou à $\frac{p^2-1}{8}$ si $a = 2$.

Le quotient de la division euclidienne de ka par p (pour $1 \leq k \leq \frac{p-1}{2}$) vaut $\left\lfloor \frac{ka}{p} \right\rfloor$. On a donc :

$$\begin{aligned} \sum_{k=1}^{(p-1)/2} ka &= \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{ka}{p} \right\rfloor + \sum_{i=1}^{n} x_i + \sum_{j=1}^{m} y_j \\ &= t_a + \sum_{i=1}^{n} x_i + \sum_{j=1}^{m} y_j. \end{aligned}$$

De plus, en se servant du fait que $\{p - x_1, \dots, p - x_n\} \cup \{y_1, \dots, y_m\} = \left\{1, \dots, \frac{p-1}{2}\right\}$, on a :

$$\sum_{k=1}^{(p-1)/2} k = \sum_{i=1}^{n} (p - x_i) + \sum_{j=1}^{m} y_j.$$

Si l'on soustrait ces deux équations, on trouve :

$$(a-1) \sum_{k=1}^{(p-1)/2} k = p(t_a - n) + 2 \sum_{i=1}^{n} x_i.$$

Or, la somme de la suite arithmétique ci-dessus vaut $\sum_{k=1}^{(p-1)/2} k = (p^2-1)/8$. Donc modulo 2 on a :

$$(a-1)\frac{p^2-1}{8} \equiv t_a - n \bmod 2.$$

Si a est impair, on trouve bien $n \equiv t_a \ [2]$.

En revanche, si $a = 2$, alors $t_2 = 0$ (car $\lfloor 2k/p \rfloor = 0$ pour tout $k \in \{1, \dots, (p-1)/2\}$) et on a bien $n \equiv (p^2-1)/8 \ [2]$. ◇

Démonstration de la loi de réciprocité quadratique. On considère l'ensemble :

$$\Lambda = \left\{ (x, y) \in \mathbb{N}^2 \;\middle|\; 1 \leq x \leq \frac{p-1}{2} \text{ et } 1 \leq y \leq \frac{q-1}{2} \right\}.$$

Il est partitionné en deux sous-ensembles (notons que l'on ne peut avoir $px = qy$) :

$$\Lambda_1 = \{(x,y) \in \Lambda \mid qx > py\}, \qquad \Lambda_2 = \{(x,y) \in \Lambda \mid qx < py\}.$$

On peut réécrire Λ_1 comme :

$$\Lambda_1 = \left\{(x,y) \in \Lambda \,\middle|\, 1 \leq x \leq \frac{p-1}{2} \text{ et } 1 \leq y < \frac{qx}{p}\right\}.$$

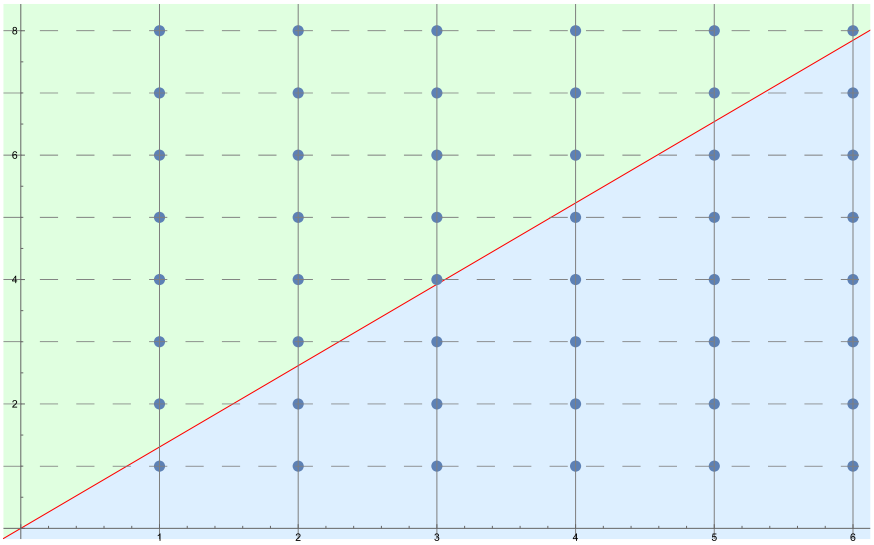


Figure I.E-c La partition de Λ en Λ_1 (en vert) et Λ_2 (en bleu) pour $p = 13$ et $q = 17$. En rouge, la droite d'équation $qx = py$.

On en déduit que le cardinal de Λ_1 vaut $\sum_{x=1}^{(p-1)/2} \lfloor qx/p \rfloor$. De façon analogue, le cardinal de Λ_2 vaut $\sum_{y=1}^{(q-1)/2} \lfloor py/q \rfloor$. La somme est le cardinal de Λ, à savoir $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$. Donc en appliquant le lemme d'Eisenstein, on obtient :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}. \qquad \diamond$$

(ii) Autre démonstration de la réciprocité quadratique

Nous allons ici présenter une des preuves de Gauss de la réciprocité quadratique. Dans la suite, on fixe un nombre premier impair p. La preuve du second complément (page 27) est légèrement plus simple et il peut être utile de la lire en premier.

Définition I.E.25. On pose $\zeta_p = e^{2i\pi/p}$ une racine primitive $p$ième de l'unité. La *somme quadratique de Gauss* $g(a,p)$ est définie, pour $a \in \mathbb{Z}$, par :

$$g(a;p) \coloneqq \sum_{n=0}^{p-1} \zeta_p^{an^2}. \qquad (*)$$

Lemme I.E.26. Si a est un entier multiple de p, on a $g(a;p) = p$.

Démonstration. En effet, si a est un multiple de p, alors $\zeta_p^{an^2} = \left(\zeta_p^a\right)^{n^2} = 1$. $\diamond$

Lemme I.E.27. Soit a un entier quelconque. Alors on a :

$$g(a;p) = \sum_{k=0}^{p-1} \left(1 + \left(\frac{k}{p}\right)\right) \zeta_p^{ak}.$$

Démonstration. D'après la **Proposition I.E.9**, il y a $\frac{p-1}{2}$ résidus quadratiques parmi $\{1, \dots, p-1\}$ et $\frac{p-1}{2}$ non-résidus. Chaque résidu quadratique apparaît donc deux fois dans la somme $(*)$. De plus $1 + \left(\frac{k}{p}\right)$ vaut 2 si $k \neq 0$ est un résidu quadratique, et 0 si c'est un non-résidu. ◇

Exemple I.E.28. Soit $p = 5$, alors :

$$\begin{aligned} g(a;5) &= 1 + \zeta_5^{1^2 a} + \zeta_5^{2^2 a} + \zeta_5^{3^2 a} + \zeta_5^{4^2 a} = 1 + \zeta_5^a + \zeta_5^{4a} + \zeta_5^{9a} + \zeta_5^{16a} \\ &= 1 + \zeta_5^a + \zeta_5^{4a} + \zeta_5^{4a} + \zeta_5^a \\ &= 1 + 2\zeta_5^a + 2\zeta_5^{4a} = 1 + 2\zeta_5^a + 0\zeta_5^{2a} + 0\zeta_5^{3a} + 2\zeta_5^{4a} \\ &= 1 + \left(1 + \left(\frac{1}{5}\right)\right)\zeta_5^a + \left(1 + \left(\frac{2}{5}\right)\right)\zeta_5^{2a} + \left(1 + \left(\frac{3}{5}\right)\right)\zeta_5^{3a} + \left(1 + \left(\frac{4}{5}\right)\right)\zeta_5^{4a}. \end{aligned}$$

Lemme I.E.29. Si a est un entier qui n'est pas divisible par p, alors on a :

$$g(a;p) = \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) \zeta_p^{ak}.$$

Démonstration. En effet, comme a est premier avec p, on a $\zeta_p^a \neq 1$, donc :

$$\sum_{k=0}^{p-1} \zeta_p^{ak} = \sum_{k=0}^{p-1} \left(\zeta_p^a\right)^k = \frac{1 - \zeta_p^{ap}}{1 - \zeta_p^a}.$$ ◇

Lemme I.E.30. Soit a un entier qui n'est pas divisible par p. On a

$$g(a;p) = \left(\frac{a}{p}\right) g(1;p).$$

Démonstration. Comme a n'est pas divisible par p, l'application $x \mapsto ax$ introduit une bijection de $\mathbb{Z}/p\mathbb{Z}$ sur lui-même. Par conséquent,

$$g(1;p) = \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) \zeta_p^k = \sum_{l=0}^{p-1} \left(\frac{al}{p}\right) \zeta_p^{al} = \sum_{l=0}^{p-1} \left(\frac{a}{p}\right)\left(\frac{l}{p}\right) \zeta_p^l = \left(\frac{a}{p}\right) g(1;p).$$ ◇

Proposition I.E.31. On a l'équation suivante :

$$g(1;p)^2 = \left(\frac{-1}{p}\right) p = (-1)^{\frac{p-1}{2}} p.$$

On rappelle que $p^* = \left(\frac{-1}{p}\right) p$. L'équation précédente dit $g(1;p)^2 = p^*$.

Démonstration. D'une part, grâce au lemme précédent, étant donné $1 \leq a \leq p-1$, on a :

$$g(a;p) g(-a;p) = \left(\frac{a}{p}\right) g(1;p) \left(\frac{-a}{p}\right) g(1;p) = \left(\frac{-1}{p}\right) g(1;p).$$

On en déduit donc que :

$$\sum_{a=1}^{p-1} g(a;p) g(-a;p) = \left(\frac{-1}{p}\right) (p-1) g(1;p).$$

D'autre part, on a :

$$g(a;p)g(-a;p) = \sum_{k=0}^{p-1}\sum_{l=0}^{p-1}\left(\frac{k}{p}\right)\left(\frac{l}{p}\right)\zeta_p^{a(k-l)}.$$

En prenant la somme sur a, on obtient :

$$\sum_{a=1}^{p-1} g(a;p)g(-a;p) = \sum_{k=0}^{p-1}\sum_{l=0}^{p-1}\left(\frac{k}{p}\right)\left(\frac{l}{p}\right)\sum_{a=1}^{p-1}\zeta_p^{a(k-l)}.$$

Or, la somme géométrique $\sum_{a=1}^{p-1}\zeta_p^{a(k-l)}$ vaut p si $k = l$ et est nulle sinon. On en déduit donc que :

$$\sum_{a=1}^{p-1} g(a;p)g(-a;p) = \sum_{k=0}^{p-1}\left(\frac{k}{p}\right)^2 p = p(p-1).$$

En combinant les deux expressions de la somme des $g(a;p)g(-a;p)$, on en déduit le résultat. ◇

Exemple I.E.32. Soit $p = 5$. On rappelle que $g(1;5) = 1 + 2\zeta_5 + 2\zeta_5^4$. On obtient donc :

$$\begin{aligned} g(1;5)^2 &= (1 + \zeta_5 + 2\zeta_5^4)^2 \\ &= 1 + 4\zeta_5^2 + 4\zeta_5^8 + 4\zeta_5 + 4\zeta_5^4 + 8\zeta_5^5 \\ &= 5 + 4(1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4) \\ &= 5. \end{aligned}$$

Démonstration du théorème. Soit $q \neq p$ un autre nombre premier impair. On a, en appliquant le critère d'Euler (**Proposition I.E.8**) :

$$g(1;p)^{q-1} = (g(1;p)^2)^{\frac{q-1}{2}} = (p^*)^{\frac{q-1}{2}} \equiv \left(\frac{p^*}{q}\right) \bmod q\,, \text{ donc :}$$

$$g(1;p)^q \equiv \left(\frac{p^*}{q}\right) g(1;p) \bmod q\,. \qquad (*)$$

Or, on peut calculer par ailleurs que (en se servant du fait que $(x+y)^q \equiv x^q + y^q \mod q$) :

$$\begin{aligned} g(1;p)^q = \left(\sum_{k=0}^{p-1}\left(\frac{t}{p}\right)\zeta_p^k\right)^q &\equiv \sum_{k=0}^{p-1}\left(\frac{t}{p}\right)\zeta_p^{kq} \bmod q \\ &\equiv g(q;p) \bmod q \\ &\equiv \left(\frac{q}{p}\right) g(1;p) \bmod q\,. \end{aligned} \qquad (**)$$

On en déduit donc, en combinant $(*)$ et $(**)$, que :

$$\left(\frac{p^*}{q}\right) g(1;p) \equiv \left(\frac{q}{p}\right) g(1;p) \bmod q.$$

Si l'on multiplie chacun des deux côtés par $g(1;p)$ et si l'on se sert du fait que $g(1;p)^2 = p^*$ est inversible modulo q, on en déduit que $\left(\frac{p^*}{q}\right) \equiv \left(\frac{q}{p}\right) \bmod q$. Comme ces deux nombres sont égaux à ± 1 et que $q \neq 2$, c'est qu'ils sont égaux. ◇

(iii) Autre démonstration du second complément

Démontrons maintenant le second complément : pour un nombre premier p donné, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. L'idée est similaire à celle de la loi de réciprocité quadratique générale, mais il faut l'adapter à la spécificité du nombre premier 2.

Posons $\zeta_8 := e^{2i\pi/8}$ une racine primitive huitième de l'unité et $\tau := \zeta_8 + \zeta_8^{-1}$. Cette « somme quadratique » satisfait une version de l'équation fondamentale des sommes quadratiques de Gauss (**Proposition I.E.31**) :

Proposition I.E.33. On a $(\zeta_8 + \zeta_8^{-1})^2 = 2$.

Démonstration. Comme $\zeta_8^2 = i$, on obtient $\zeta_8^2 + \zeta_8^{-2} = 0$, ce qui permet d'avoir :

$$\tau^2 = \zeta_8^2 + 2 + \zeta_8^{-2} = 2 + 0 = 2. \qquad \diamond$$

Démonstration du théorème. On peut maintenant démontrer le complément d'une manière analogue à la preuve de la réciprocité quadratique. D'une part, grâce au critère d'Euler, on a :

$$\tau^{p-1} = (\tau^2)^{\frac{p-1}{2}} = 2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \bmod p\,, \text{ donc :}$$

$$\tau^p \equiv \left(\frac{2}{p}\right)\tau \bmod p\,. \qquad (*)$$

Par ailleurs, on a :

$$\tau^p = (\zeta_8 + \zeta_8^{-1})^p \equiv \zeta_8^p + \zeta_8^{-p} \bmod p.$$

Il y a deux cas possibles :

- Si $p \equiv \pm 1 \bmod 8$, alors $\zeta_8^p + \zeta_8^{-p} = \zeta_8 + \zeta_8^{-1} = \tau = (-1)^{\frac{p^2-1}{8}}\tau$.
- Sinon (si $p \equiv \pm 3 \bmod 8$), $\zeta_8^p + \zeta_8^{-p} = -\tau = (-1)^{\frac{p^2-1}{8}}\tau$.

Donc quoi qu'il en soit, $\tau^p \equiv (-1)^{\frac{p^2-1}{8}}\tau \bmod p$. En combinant avec $(*)$, on trouve

$$\left(\frac{2}{p}\right)\tau \equiv (-1)^{\frac{p^2-1}{8}}\tau \bmod p.$$

Si on multiplie chacun des deux côtés de cette congruence par τ et si on note que $\tau^2 = 2$ est inversible mod p, on trouve que $\left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}} \bmod p$. Or ces deux nombres sont égaux à ± 1 et $p \neq 2$; c'est donc que les deux nombres sont égaux. $\diamond$

§ I.E(c) Symbole de Jacobi

Le symbole de Legendre $\left(\frac{a}{p}\right)$ n'est défini que si p est un nombre premier impair. Il existe une généralisation, le symbole de Jacobi, qui est défini si la deuxième variable est un nombre entier impair arbitraire. Son intérêt principal est de fournir un algorithme rapide pour calculer le symbole de Legendre.

Définition I.E.34. Soit $n = \prod_{i=1}^{k} p_i$ un entier *impair* et sa décomposition en facteurs premiers (non nécessairement distincts), et soit $a \in \mathbb{Z}$ un entier quelconque. Le *symbole de Jacobi* $\left(\frac{a}{n}\right)$ est défini par :

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right).$$

Remarque I.E.35. Étant donné $a \in \mathbb{Z}$, le nombre $\left(\frac{a}{1}\right)$ est un produit vide et vaut donc 1.

Remarque I.E.36. Si n est un nombre premier impair alors $\left(\frac{a}{n}\right)$ est égal au symbole de Legendre.

Les propriétés suivantes sont faciles à vérifier.

Proposition I.E.37. Le symbole de Jacobi $\left(\frac{a}{n}\right)$ ne dépend que de la classe de a modulo n.

Remarque I.E.38. Le symbole de Jacobi $\left(\frac{a}{n}\right)$ est non-nul si et seulement si $a \wedge n = 1$.

Proposition I.E.39. Le symbole de Jacobi est complètement multiplicatif en chaque variable, c'est-à-dire que pour tous $a, b \in \mathbb{Z}$ et tous $m, n \in \mathbb{N}$ impairs, on a :

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right), \qquad \left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right).$$

Remarque I.E.40. En particulier, quels que soient a et n (impair) premiers entre eux, $\left(\frac{a}{n^2}\right) = 1$.

Avertissement I.E.41. Étant donnés a et n, même si $\left(\frac{a}{n}\right) = 1$, il est possible que a ne soit pas un résidu quadratique mod n. Par exemple, $\left(\frac{5}{9}\right) = \left(\frac{5}{3}\right)^2 = 1$ alors que 5 n'est pas un résidu quadratique mod 9. En revanche, si $\left(\frac{a}{n}\right) = -1$, alors a ne peut pas être un résidu quadratique modulo n.

Proposition I.E.42. Le symbole de Jacobi vérifie les relations suivantes, qui généralisent la réciprocité quadratique, pour tous a, b entiers naturels impairs :

$$\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}, \qquad \left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}, \qquad \left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\left(\frac{a-1}{2}\right)\left(\frac{b-1}{2}\right)}.$$

Lemme I.E.43. Soit r, s des entiers impairs. Alors on a :

$$\frac{rs-1}{2} \equiv \frac{r-1}{2} + \frac{s-1}{2} \bmod 2,$$
$$\frac{r^2s^2-1}{8} \equiv \frac{r^2-1}{8} + \frac{s^2-1}{8} \bmod 2.$$

Pour le premier énoncé, notons que $r-1$ et $s-1$ sont pairs, donc :

$$\begin{aligned}(r-1)(s-1) &\equiv 0 \bmod 4\\ \Longrightarrow rs-1 &\equiv r-1+s-1 \bmod 4\\ \Longrightarrow \frac{rs-1}{2} &\equiv \frac{r-1}{2} + \frac{s-1}{2} \bmod 2.\end{aligned}$$

Le raisonnement est le même pour le deuxième énoncé en notant que r^2-1 et s^2-1 sont divisibles par 4. ◇

Démonstration de la proposition. Posons $a = p_1 \dots p_m$ et $b = q_1 \dots q_n$ les décompositions en facteurs premiers de a et b. Alors on a, en appliquant le lemme plusieurs fois par récurrence :

$$\left(\frac{-1}{b}\right) = \left(\frac{-1}{q_1}\right) \dots \left(\frac{-1}{q_n}\right) = (-1)^{\frac{q_1-1}{2}+\dots+\frac{q_n-1}{2}} = (-1)^{\frac{q_1 \dots q_m-1}{2}} = (-1)^{\frac{b-1}{2}}.$$

De la même manière, $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$. Enfin,

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = \prod_{i,j}\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = (-1)^{\sum_{i,j}\left(\frac{p_i-1}{2}\right)\left(\frac{q_j-1}{2}\right)} = (-1)^{\left(\frac{a-1}{2}\right)\left(\frac{b-1}{2}\right)}.$$ ◇

Remarque I.E.44. Ces propriétés permettent de trouver un algorithme efficace pour calculer le symbole de Jacobi [2, section 31].

Section I.F. Tests de primalité

§ I.F(a) Test de Fermat

Nous avons vu dans la Section I.C un premier test de (non-)primalité : étant donné un entier n, on choisit au hasard un entier $2 \leq a \leq n-1$ et on teste deux choses :

- Est-ce que a et n sont premiers entre eux ? On peut calculer rapidement leur PGCD par l'algorithme d'Euclide. S'ils ne sont pas premiers entre eux, alors n n'est pas premier.
- Est-ce que $a^{n-1} \equiv 1 \mod n$, ou pas ?

Si $a \wedge n = 1$ mais que l'équation est fausse, n n'est pas premier et on dit que a est un témoin de Fermat de n. Si elle est vraie, au contraire, alors n est probablement premier. Pour un algorithme plus précis, on peut répéter l'opération un nombre fixé de fois (on choisit k nombres $a_1, \dots, a_k$ au hasard et on réalise le test). En Mathematica :

```
testFermat[n_] /; n >= 3 := Module[{a, an, d},
  a = RandomInteger[{2, n}];
  d = euclide[a, n];
  d == 1 &&
   PowerMod[a, n - 1, n] == 1
  ]
```

Il n'est en général pas nécessaire de considérer *tous* les entiers inférieurs à p dans le test. À titre d'indication, il n'existe que 21 853 nombres p inférieurs à $2{,}5 \times 10^{10}$ qui ne sont pas premiers mais tels que 2^p est congru à 2 modulo p (voir [9]).

Remarque I.F.1. Si l'on connaît un témoin de Fermat pour un entier n, on sait qu'il est composé, mais le témoin ne nous donne pas de factorisation. Il s'agit simplement d'un « certificat » de non-primalité.

Cependant, cet algorithme n'est pas très efficace d'un point de vue algorithmique : sa complexité temporelle est de l'ordre de $O(\ln^2(p)\ln(ln(p)))$. Il est par ailleurs d'une précision limitée. Étant donné $a \geq 2$, il existe une infinité d'entiers n composés tels que $a^{n-1} \equiv 1 \mod n$, appelés « nombres pseudo-premiers de Fermat en base a » et a est appelé un *menteur de Fermat* pour n.

Exemple I.F.2. Considérons $n = 2373$. On vérifie facilement que n n'est pas premier : par exemple, $2^{2372} \equiv 2083 \mod n$ est un témoin de Fermat (en fait, $n = 3 \times 7 \times 113$). Mais il existe 15 menteurs de Fermat (211, 566…).

Pire encore, il existe des nombres qui sont pseudo-premiers en toute base !

Théorème I.F.3 (Korselt). Soit $n > 2$ un entier. Les propositions suivantes sont équivalentes :

- Pour tout entier a premier avec n, on a $a^{n-1} \equiv 1 \mod n$.
- Le nombre n n'a aucun facteur carré, et si p est un facteur premier de n, $p-1$ divise $n-1$.

Démonstration. Supposons d'abord que n vérifie la première propriété. Si n avait un facteur carré, disons $n = p^\alpha n'$ où $\alpha \geq 2$ et $p \wedge n' = 1$, nous allons démontrer qu'on arrive à une contradiction. D'après le théorème des restes chinois, on a $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p^\alpha\mathbb{Z})^\times \times (\mathbb{Z}/n'\mathbb{Z})^\times$. Soit $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ la classe qui correspond à $(1+p, 1)$ (c'est-à-dire $a \equiv 1+p \mod p^\alpha$ et $a \equiv 1 \mod n'$). En particulier, $a \equiv 1+p \mod p^2$. Alors a est premier avec p^α et avec n', donc avec $n = p^\alpha \vee n'$, et donc par hypothèse $a^{n-1} \equiv 1 \mod n$. Mais par ailleurs, modulo p^2, on trouve :

$$\begin{aligned} a^{n-1} &\equiv (1+p)^{n-1} \mod p^2 \\ &\equiv 1 + (n-1)p \mod p^2 \\ &\equiv 1 - p \mod p^2. \end{aligned}$$

On trouve donc $1 \equiv 1 - p \mod p^2$, ce qui est absurde.

Démontrons maintenant que si $p \mid n$ est un diviseur premier de n alors $p-1 \mid n-1$. Soit $b \in (\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/(p-1)\mathbb{Z}$ un générateur et posons $n = pn'$. D'après ce qui précède, $p \wedge n' = 1$, donc d'après le théorème des restes chinois, $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/n'\mathbb{Z})^\times$. Choisissons $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ la classe qui correspond à $(b, 1)$. On a $a^{n-1} \equiv 1 \mod n$ par hypothèse, ce qui donne $b^{n-1} \equiv 1 \mod p$. Comme b est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$, son ordre vaut $p-1$, donc $p-1 \mid n-1$.

Supposons maintenant que $n = p_1 \dots p_k$ n'a pas de facteur carré et $p_i - 1 \mid n-1$ pour tout i. Soit a un entier premier à n. En particulier, pour chaque i, $a \wedge p = 1$, donc on a $a^{p_i - 1} \equiv 1 \ [p_i]$. Or, $p_i - 1 \mid n - 1$, donc $a^{n-1} \equiv 1 \ [p_i]$. Or d'après le théorème des restes chinois, $(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_i (\mathbb{Z}/p_i\mathbb{Z})^\times$ (car tous les p_i sont premiers entre eux), donc en regroupant toutes les congruences, on arrive bien à l'équation voulue, $a^{n-1} \equiv 1 \ [n]$. ◇

Définition I.F.4. Un *nombre de Carmichael* est un entier composé n tel que pour tout entier a premier avec n, on ait $a^{n-1} \equiv 1 \ [n]$.

Théorème I.F.5 (Alford–Granville–Pomerance [1])**.** Il existe une infinité de nombres de Carmichael.

Exemple I.F.6. Le plus petit nombre de Carmichael est $561 = 3 \times 11 \times 17$.

Exemple I.F.7. Soit m un entier tel que $6m+1$, $12m+1$ et $18m+1$ soient premiers. Alors $n = (6m+1)(12m+1)(18m+1)$ est un nombre de Carmichael.

Ces contre-exemples empêchent le test de Fermat d'être un test de primalité à proprement parler. Bien que les nombres de Carmichael soient rares comparés aux nombres premiers, ils ne sont pas un cas isolé : il est possible qu'un nombre n ne possède que très peu de témoins de Fermat, même s'il n'est pas un nombre de Carmichael.

Le test de Fermat a pour complexité temporelle[5] $O(\ln^2(p) \ln(ln(p)))$ et reste utilisé comme premier test de primalité dans les bibliothèques cryptographiques modernes, malgré son imprécision. Dans cette section, nous allons voir d'autres algorithmes plus efficaces et/ou plus précis.

[5] En utilisant un algorithme d'exponentiation modulaire rapide pour le calcul de $a^p \mod p$.

§ I.F(b) Test de Solovay–Strassen

Le test de Solovay–Strassen utilise le critère d'Euler (**Proposition I.E.8**), qui dit qu'étant donné un nombre premier $p > 2$ et un entier a, on a :

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p.$$

Le test consiste alors, étant donné un nombre impair n, à choisir (au hasard) un nombre a, et à vérifier si $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \bmod n$ ou non. Si l'équation est fausse, alors n n'est pas premier et on appelle a un *témoin d'Euler* pour n ; si elle est vraie, alors n est *probablement* premier. En Mathematica :

```
testSolovayStrassen[n_] /; n >= 3 := Module[{a, an, d},
  a = RandomInteger[{2, n}];
  d = euclide[a, n];
  d == 1 &&
   Divisible[PowerMod[a, (n - 1)/2, n] - JacobiSymbol[a, n], n]
  ]
```

Comme avec le test de Fermat (et tous les tests probabilistes), il est possible que le test de Solovay–Strassen dise qu'un nombre est probablement premier sans qu'il soit premier. On dit que a est un *menteur d'Euler* pour n, ou que n est un nombre *pseudo-premier d'Euler–Jacobi* » en base a, si n est composé et impair, que $a \wedge n = 1$, mais que $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \bmod n$.

Exemple I.F.8. Le nombre $n = 561$ est composé. Le nombre 5 est un témoin d'Euler, car $5^{280} \equiv 67 \bmod 561$ n'est pas congru au symbole de Jacobi $\left(\frac{5}{561}\right)$. Cependant, il y a plusieurs menteurs d'Euler, par exemple $a = 2$ (car $2^{280} \equiv 1 \bmod 561$ et $\left(\frac{2}{561}\right) = 1$).

Si l'on utilise l'exponentiation rapide, ce test est moins efficace temporellement que le test de Fermat : il a une complexité temporelle de $O(\ln^3(n))$, et $\ln^3(n) \gg \ln^2(n)\ln(ln(n))$ quand $n \to \infty$. Il existe néanmoins des versions modernes de la multiplication modulaire [10] qui utilisent la transformée de Fourier rapide, ce qui permet d'obtenir un algorithme de complexité temporelle $O(\ln^2(n))$, meilleure que le test de Fermat.

Ce test est également plus précis que le test de Fermat. Par exemple, l'analogue des nombres de Carmichael n'existe pas, et chaque nombre composé n possède de nombreux témoins d'Euler.

Lemme I.F.9. Si a est un témoin de Fermat pour n, alors c'est un témoin d'Euler.

Théorème I.F.10 (Solovay–Strassen [11]**).** Tout nombre composé a au moins un témoin d'Euler.

Démonstration. Soit n un entier composé et supposons un instant que n n'a pas de témoin d'Euler. Il n'a donc pas de témoin de Fermat, en d'autres termes, c'est un nombre de Carmichael. D'après le théorème de Korselt, on peut donc écrire $n = p_1 \dots p_k$ comme un produit de facteurs premiers distincts ($k \geq 2$), et pour tout i, on a $p_i - 1 \mid n - 1$.

Quitte à échanger, on peut supposer $p_1 \neq 2$. Il existe au moins un nombre b qui n'est pas un résidu quadratique modulo p_1. D'après le théorème des restes chinois, on peut trouver $a \in \mathbb{Z}/n\mathbb{Z}$ tel que l'on ait :

$$a \equiv b \ (\bmod p_1), \qquad a \equiv 1 \ (\bmod p_2 \dots p_k).$$

On a donc $\left(\frac{a}{p_1}\right) = -1$ et $\left(\frac{a}{p_i}\right) = 1$ pour $i \geq 2$, donc $\left(\frac{a}{n}\right) = -1$. Mais par ailleurs, on a $a^{\frac{p_2-1}{2}} \equiv 1 \mod p_2$ d'après le critère d'Euler. Comme $p_2 - 1 \mid n - 1$, on en déduit $a^{\frac{n-1}{2}} \equiv 1 \mod p_2$. C'est donc que a est un témoin d'Euler pour n, ce qui contredit l'hypothèse initiale. ◇

Lemme I.F.11. L'ensemble des menteurs d'Euler d'un entier impair n forme un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^\times$.

Démonstration. En effet, 1 est bien un menteur d'Euler ($1^{\frac{n-1}{2}} = 1 = \left(\frac{1}{n}\right)$) et si a, b sont deux menteurs d'Euler, on a :

$$(ab)^{\frac{n-1}{2}} = a^{\frac{n-1}{2}} b^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right)\left(\frac{b}{n}\right) = \left(\frac{ab}{n}\right) \mod n\,.$$ ◇

Corollaire I.F.12. Si n est un nombre composé, alors au moins la moitié des éléments de $(\mathbb{Z}/n\mathbb{Z})^\times$ sont des témoins d'Euler de n.

Démonstration. L'ensemble M des menteurs d'Euler est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^\times$. Comme n est composé, il s'agit d'un sous-groupe strict, d'indice $d \geq 2$. On a donc $|M| = \frac{|(\mathbb{Z}/n\mathbb{Z})^\times|}{d} \leq \frac{n-1}{2}$, donc il y a au moins $\frac{n-1}{2}$ témoins d'Euler de n. ◇

§ I.F(c) Test de Miller–Rabin

Le test de Solovay–Strassen n'est plus utilisé dans les bibliothèques cryptographiques modernes et a été remplacé par deux tests plus récents, le test Baillie–PSW et le test de Miller–Rabin. Terminons ce chapitre par la description du test de Miller–Rabin, qui allie rapidité et simplicité.

Soit $n \geq 3$ un entier impair. On peut écrire $n - 1 = 2^s m$, où $s > 0$ et m est impair. On choisit au hasard un entier $a \in \{2, \dots, n-2\}$ premier avec n, on teste si l'une des congruences suivantes est vérifiée :

$$a^m \equiv 1 \ [n], \qquad \exists r \in \{0, \dots, s-1\}, a^{2^r m} \equiv -1 \mod n.$$

Si aucune de ces congruences n'est vraie, alors n n'est pas premier (voir le lemme suivant) et on appelle a un *témoin fort* pour n. Si au moins l'une d'elles est vraie, alors n est *probablement* premier. Comme pour les autres tests, si n est composé, on appelle alors a un *menteur fort*. En Mathematica :

```
testMillerRabin[n_] := Module[{a, s, m, apowm, l},
  a = RandomInteger[{2, n - 2}];
  s = IntegerExponent[n - 1, 2];
  m = (n - 1)/2^s;
  apowm = PowerMod[a, m, n];
  (* {apowm, apowm^2, apowm^4, ..., apowm^(2^s)} *)
  l = NestList[PowerMod[#, 2, n] &, apowm, s];
  PowerMod[a, m, n] == 1 || MemberQ[l, n - 1]
]
```

Lemme I.F.13. Soit $n \geq 3$ un entier impair, et posons $n - 1 = 2^s m$ où m est impair. Supposons qu'il existe un entier a premier à n tel que toutes les inéquations suivantes soient vérifiées modulo n :

$$a^m \not\equiv 1 \ (\mathrm{mod}\, n), \qquad a^{2^0 m} \not\equiv -1 \ (\mathrm{mod}\, n), \qquad a^{2^1 m} \not\equiv -1 \ (\mathrm{mod}\, n), \qquad \dots, \qquad a^{2^{s-1} m} \not\equiv -1 \ (\mathrm{mod}\, n).$$

Alors n est composé.

Démonstration. Supposons qu'un tel a existe et que n est premier. D'après le petit théorème de Fermat, on a alors $a^{2^s m} = a^{n-1} \equiv 1 \mod n$. Posons $x = a^m$. Les inéquations ci-dessus deviennent :

$$x \not\equiv \pm 1 \pmod n, \qquad x^2 \not\equiv -1 \pmod n, \qquad (x^2)^2 \not\equiv -1 \pmod n, \qquad \dots, \qquad x^{2^{s-1}} \not\equiv -1 \pmod n.$$

Or, $x^{2^{s-1}}$ est une racine carrée de $x^{2^s} = a^{n-1} \equiv 1 \mod n$. Comme n est premier, le nombre 1 n'a que deux racines carrées $\mod n$, à savoir ± 1. Comme par hypothèse $x^{2^{r-1}} \not\equiv -1 \pmod n$, c'est qu'en fait $x^{2^{r-1}} \equiv 1 \mod n$. En continuant ainsi de proche en proche (formellement, par récurrence), on en arrive à $x^2 \equiv 1 \pmod n$. Donc x est une racine carrée de $1 \bmod n$. Mais par hypothèse, $x \not\equiv \pm 1\ [n]$, c'est absurde. ◇

Exemple I.F.14. Tentons de déterminer si $n = 377$ est premier ou non.

- On commence par factoriser $n - 1 = 377 = 2^3 \times 47$, c'est-à-dire $s = 3$ et $m = 47$.
- Choisir a au hasard ; par exemple $a = 99$;
- Calculer $b = a^{47} \bmod n$; ici, $b \equiv 278 \mod 377$;
- Comme b ne vaut ni 1 ni -1, on continue ;
- Calculer ses carrés successifs (b^2, $(b^2)^2 = b^{2^2}$,$((b^2)^2)^2 = b^{2^3}$) jusqu'à ce qu'on en trouve un congru à -1 ; ici $b^2 \equiv -1 \mod 577$, on s'arrête : 577 est probablement premier.

Pour plus de certitude, appliquons à nouveau l'algorithme, cette fois-ci avec $a = 31$. Maintenant, les classes de (b, b^2, b^4, b^8) sont $(229, 38, 313, 326)$. La première n'est pas congrue à ± 1 et les suivantes ne sont pas congrues à -1. Donc a est un témoin fort pour $n = 377$ qui est composé, et 99 était un menteur fort ! On a en fait $377 = 13 \times 29$. Mais comme pour les tests de primalité précédents, le test de Miller–Rabin ne fournit que des certificats de non-primalité, sans donner une décomposition du nombre n.

La borne supérieure sur le nombre de menteurs forts pour le test Rabin–Miller est meilleure que pour le test de Solovay–Strassen :

Proposition I.F.15. Soit n un entier composé. Il existe au plus $\varphi(n)/4$ menteurs forts pour n.

Concluons par une comparaison des trois tests.

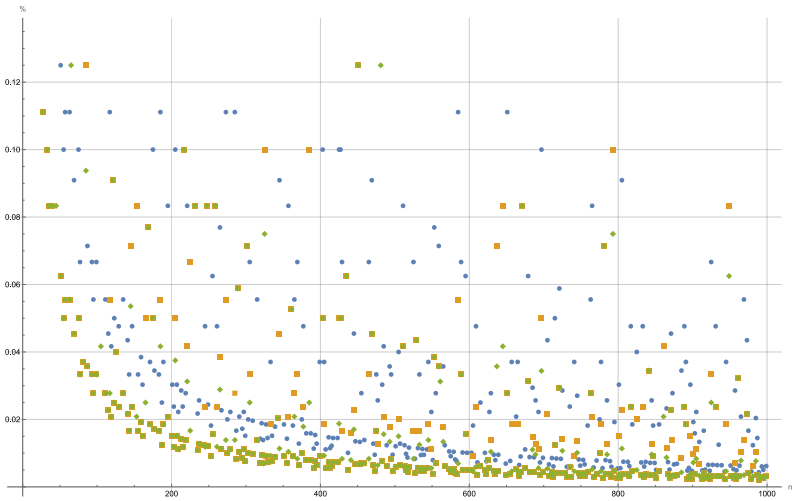


Figure I.F-a Le ratio des menteurs de Fermat (cercles bleus), des menteurs d'Euler (carrés oranges) et des menteurs forts (losanges verts), parmi l'ensemble des nombres premiers à un entier n donné. Les tests de Solovay–Strassen et Rabin–Miller sont toujours meilleurs que le test de Fermat. Ces deux tests sont souvent d'aussi bonne précision, mais le test de Rabin–Miller bat parfois celui de Solovay–Strassen.

Chapitre II. THÉORIE DES ANNEAUX

« Un Anneau pour les gouverner tous. »

J. R. R. Tolkien, *Le Seigneur des Anneaux*

Le chapitre précédent concernait les propriétés algébriques de l'anneau $\mathbb{Z}$ et de ses quotients. Dans ce chapitre, nous allons généraliser une partie des propriétés de $\mathbb{Z}$ à d'autres anneaux.

Section II.A. Généralités sur les anneaux

§ II.A(a) Anneaux, idéaux

Définition II.A.1. Un *anneau* est la donnée d'un groupe abélien $(A, +, 0)$ muni d'une fonction bilinéaire associative $A \times A \to A$, $(x, y) \mapsto xy$ (le produit de l'anneau) et d'une unité $1 \in A$. L'anneau est dit *commutatif* si la multiplication bilinéaire l'est. Un *morphisme d'anneaux* est une fonction $f : A \to B$ entre deux anneaux qui est un morphisme de groupes abéliens pour l'addition et qui vérifie $f(1) = 1$ et $f(aa') = f(a)\, f(a')$ pour tous $a, a' \in A$.

Convention II.A.2. Désormais, tous les anneaux seront supposés commutatifs, sauf mention contraire. La théorie des anneaux non-commutatifs est passionnante mais dépasse le cadre de ce que l'on présentera ici.

Exemple II.A.3. Les anneaux classiques sont $\mathbb{Z}$ (entiers), $\mathbb{Q}$ (rationnels), $\mathbb{R}$ (réels), $\mathbb{C}$ (complexes).

Exemple II.A.4. L'ensemble $\mathbb{Z}[i] = \{x + iy \in \mathbb{C} \mid x, y \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{C}$. On l'appelle l'anneau des *entiers de Gauss*.

Exemple II.A.5. Les fonctions continues sur $\mathbb{R}$ forment un anneau $\mathcal{C}(\mathbb{R})$.

Remarque II.A.6. Soit A un anneau. Il existe un unique morphisme d'anneaux $f : \mathbb{Z} \to A$. Pour $n \geq 0$ un entier, il est donné par :

$$f(n) = f(1 + 1 + \cdots + 1) = f(1) + f(1) + \cdots + f(1).$$

Si $n < 0$, on a de plus $f(-n) = -f(n)$. On note en général $n \cdot 1 \coloneqq f(n)$.

Définition II.A.7. Un *idéal* I d'un anneau A est un sous-ensemble non-vide, stable par l'addition, et tel que $\forall a \in A, \forall x \in I, ax \in I$. Étant donné une famille $(a_1, \ldots, a_n, \ldots)$ d'éléments de A (potentiellement infinie), on note $(a_1, \ldots, a_n, \ldots)$ le plus petit idéal contenant les a_i et on l'appelle l'*idéal engendré* par la famille.

Définition II.A.8. Le *quotient* d'un anneau A par un idéal I est noté A/I.

Proposition II.A.9. Soit A et $a_1, \ldots, a_n, \ldots \in A$ des éléments. L'idéal $(a_1, \ldots, a_n, \ldots)$ est l'ensemble des combinaisons linéaires finies des a_i :

$$(a_1, \ldots, a_n) = \{\textstyle\sum_i \lambda_i a_i \mid \lambda_i \in A, \text{ seul un nombre fini de } \lambda_i \text{ sont non-nuls}\}.$$

Exemple II.A.10. L'ensemble $\mathbb{Z}$ muni de l'addition et de la multiplication est un anneau commutatif. Étant donné $n \in \mathbb{Z}$, le sous-groupe $n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\} = (n)$ est un idéal de $\mathbb{Z}$. Le quotient $\mathbb{Z}/n\mathbb{Z}$ est l'anneau des entiers modulo n.

Exemple II.A.11. Soit $f : A \to B$ un morphisme d'anneaux. Le noyau $\ker(f)$ est un idéal de A. L'image $\mathrm{im}(f)$ est un sous-anneau de B.

Proposition II.A.12. Un morphisme d'anneaux $f : A \to B$ induit un isomorphisme $A/\ker(f) \to \mathrm{im}(f)$.

Proposition II.A.13. Soit A un anneau et I un idéal. Les idéaux de A/I sont en bijection avec les idéaux de A contenant I.

Proposition II.A.14. Soit I, J deux idéaux d'un anneau A. Leur intersection $I \cap J$ est encore un idéal et on a :

$$I \cap J = IJ \coloneqq \{ x_1 y_1 + \cdots + x_n y_n \mid x_k \in I,\ y_k \in J \}.$$

Leur somme, $I + J$ (définie de façon analogue) est également un idéal. C'est le plus petit idéal qui contient à la fois I et J.

§ II.A(b) Éléments inversibles

Définition II.A.15. Soit A un anneau. On dit que $a \in A$ est *inversible* s'il existe $b \in A$ avec $ab = 1$. On note $A^\times$ l'ensemble des éléments inversibles de A, c'est-à-dire :

$$A^\times \coloneqq \{ a \in A \mid \exists b \in A,\ ab = 1 \}.$$

Cet ensemble forme un groupe pour la multiplication.

Avertissement II.A.16. Il ne faut pas confondre cette notation avec les notations $\mathbb{N}^*, \mathbb{Z}^*$ … introduites précédemment ! La notation $\mathbb{N}^\times$ n'aurait pas de sens car $\mathbb{N}$ n'est pas un anneau[6]. Seuls deux éléments de $\mathbb{Z}$ sont inversibles : $\mathbb{Z}^\times = \{1, -1\} \neq \mathbb{Z}^*$. En revanche, on a bien $\mathbb{Q}^\times = \mathbb{Q}^*$, $\mathbb{R}^\times = \mathbb{R}^*$ et $\mathbb{C}^\times = \mathbb{C}^*$.

Remarque II.A.17. On a déterminé $(\mathbb{Z}/n\mathbb{Z})^\times$ au chapitre précédent.

Exercice II.A.18. Déterminer le groupe $\mathbb{Z}[i]^\times$.

Proposition II.A.19. Un élément $a \in A$ est inversible si et seulement si $(a) = A$.

Nous étudierons les corps plus en détail dans le Chapitre III. Énonçons ici quelques propriétés de base à leur sujet.

Définition II.A.20. Un *corps* est un anneau commutatif tel que $0 \neq 1$ et tout élément non-nul est inversible.

Remarque II.A.21. Un anneau A est un corps si et seulement si $A^\times = A \setminus \{0\}$.

Exemple II.A.22. L'anneau $\mathbb{Z}$ des entiers n'est pas un corps : 2 n'a pas d'inverse pour la multiplication. L'anneau $\mathbb{Q}$ des nombres rationnels, l'anneau $\mathbb{R}$ des nombres réels, et l'anneau $\mathbb{C}$ des nombres complexes sont tous les trois des corps.

Exercice II.A.23. Si $\mathbb{K}$ est un corps, montrer que $\mathbb{K}[X]^\times = \mathbb{K}^\times$. Trouver un élément inversible non-constant dans $(\mathbb{Z}/4\mathbb{Z})[X]$.

Proposition II.A.24. Soit $f : A \to B$ un morphisme d'anneaux. Si A est un corps et si B n'est pas l'anneau nul, alors f est injectif.

[6] Il s'agit néanmoins d'un « demi-anneau ». On peut définir l'ensemble des inversibles d'un demi-anneau et on a alors $\mathbb{N}^\times = \{1\}$.

Démonstration. Supposons que $x \in A$ est un élément non-nul. Alors x admet un inverse x^{-1} avec $xx^{-1} = 1$. Donc $f(xx^{-1}) = 1 = f(x)\,f(x^{-1})$. Comme $1 \neq 0$ dans B, on ne peut donc pas avoir $f(x) = 0$. ◇

Corollaire II.A.25. Tout morphisme entre deux corps est injectif.

§ II.A(c) Polynômes

Les anneaux de polynômes seront étudiés plus en détails dans la Section II.D. Donnons ici simplement les définitions de base qui les concernent.

Définition II.A.26. Soit A un anneau. On note $A[X]$ *l'anneau des polynômes* en une variable X à coefficients dans A.

Formellement, on peut définir $A[X]$ comme l'ensemble des suites à support fini :

$$A[X] \coloneqq \{\,(a_n)_{n\geq 0} \mid \exists d \in \mathbb{N},\ \ \forall n \geq d,\ \ a_n = 0\,\}.$$

Cet ensemble est muni de l'addition et de la multiplication suivantes :

$$(a_n)_{n\geq 0} + (b_n)_{n\geq 0} \coloneqq (a_n + b_n)_{n\geq 0},$$
$$(a_n)_{n\geq 0} \cdot (b_n)_{n\geq 0} \coloneqq \left(\sum_{k+l=n} a_k b_l\right)_{n\geq 0}.$$

L'élément nul est la suite constante $(0, 0, \dots)$ et l'unité est la suite $(1, 0, 0, \dots)$. L'identification avec le point de vue usuel sur les polynômes se fait en considérant une suite comme la suite des coefficients d'un polynôme :

$$\sum_{n=0}^{\infty} a_n X^n = a_0 X^0 + a_1 X^1 + a_2 X^2 + \cdots \coloneqq (a_n)_{n\geq 0} \in A[X].$$

On définit également l'anneau des polynômes en plusieurs variables par récurrence :

$$A[X_1, \dots, X_n] \coloneqq (A[X_1, \dots, X_{n-1}])[X_n].$$

§ II.A(d) Algèbres

Définition II.A.27. Soit A un anneau. Une *A-algèbre* est la donnée d'un couple (B, f) où B est un anneau et $f\colon A \to B$ est un morphisme. Un *morphisme de A-algèbre* $\varphi\colon (B, f) \to (C, g)$ est un morphisme d'anneaux $\varphi\colon B \to C$ tel que $\varphi \circ f = g$.

Remarque II.A.28. En règle générale, on note simplement une algèbre B et le morphisme f est tacite.

Remarque II.A.29. Tout anneau possède une unique structure de $\mathbb{Z}$-algèbre.

Exemple II.A.30. L'anneau $A[X_1, \dots, X_n]$ est une A-algèbre avec le morphisme évident $A \to A[X_1, \dots, X_n]$.

L'algèbre $A[X]$ est caractérisé par la propriété « universelle » suivante.

Proposition II.A.31. Soit A un anneau, B une A-algèbre et $b \in A$. Il existe un unique morphisme de A-algèbres $A[X] \to B$, appelé *évaluation* en a et noté $P \mapsto P(b)$, tel que $X \mapsto b$.

Démonstration. Notons $f\colon A \to B$ le morphisme structurel. Étant donné $P = \sum_{i=0}^{n} a_i X^i \in A[X]$, on définit :

$$P(b) \coloneqq \sum_{i=0}^{n} f(a_i) b^i.$$

On vérifie aisément que cela définit un morphisme de A-algèbres tel que $X \mapsto b$, et que ce morphisme est l'unique à vérifier ces propriétés. ◇

Remarque II.A.32. Par récurrence, étant donné une A-algèbre B et des éléments $b_1, \dots, b_n \in B$, il existe un unique morphisme $A[X_1, \dots, X_n] \to B$ tel que $X_i \mapsto b_i$.

Définition II.A.33. Une *racine* d'un polynôme $P \in A[X]$ est un élément $a \in A$ tel que $P(a) = 0 \in A$.

Remarque II.A.34. En général, on ne peut pas identifier les polynômes à coefficients dans A avec des fonctions $A \to A$, contrairement avec ce dont on a l'habitude quand $A = \mathbb{R}$. Considérons $P = X^2 + X$ vu comme un polynôme à coefficients dans $\mathbb{Z}/2\mathbb{Z}$. Ce polynôme n'est pas l'élément nul de $(\mathbb{Z}/2\mathbb{Z})[X]$. Cependant, quel que soit $a \in \mathbb{Z}/2\mathbb{Z}$, on a $P(a) = 0$.

Définition II.A.35. Une A-algèbre B est dite de *type fini* si elle est engendrée en tant qu'algèbre par un nombre fini d'éléments $b_1, \dots, b_n$. Cela revient à demander que l'unique morphisme de A-algèbres $A[X_1, \dots, X_n] \to B$ déterminé par $X_i \mapsto b_i$ soit surjectif, ou encore que B soit un quotient d'une algèbre polynomiale.

Définition II.A.36. Soit A un anneau et B une A-algèbre. Soit $b \in B$ un élément. On note $A[b]$ la *sous-algèbre (de B) engendrée par b*. Il s'agit de la plus petite sous-A-algèbre de B qui contient b. Elle est égale à l'image du morphisme $A[X] \to B$ qui envoie X sur b.

Plus généralement, si $E \subset B$ est un sous-ensemble, on note $A[E]$ la *sous-algèbre (de B) engendrée par E*. C'est l'image de l'unique morphisme $A[X_b]_{b \in E} \to B$ qui envoie X_b sur $b \in E \subset B$.

Exemple II.A.37. Vérifier que $\mathbb{Z}[i] = \{ a + bi \mid a, b \in \mathbb{Z} \}$, où $i \in \mathbb{C}$ est l'unité imaginaire.

Remarque II.A.38. Cet exemple montre qu'en général, l'anneau $A[b]$ n'est pas isomorphe à l'anneau de polynômes $A[X]$.

Section II.B. Propriétés des anneaux

Dans cette section, on introduit plusieurs propriétés des anneaux, de plus en plus exigeantes (sauf la notion d'anneau noethérien qui n'est pas au programme). Les imbrications entre ces différentes classes d'anneaux est résumée par :

$$\text{euclidien} \implies \text{principal} \implies \text{factoriel} \implies \text{intègre}.$$

§ II.B(a) Anneaux intègres

Définition II.B.1. Soit A un anneau et $a \in A \setminus \{0\}$ un élément non nul. On dit que a est un *diviseur de zéro* s'il existe $b \in A \setminus \{0\}$ tel que $ab = 0$.

Exemple II.B.2. Dans l'anneau $\mathbb{Z}/4\mathbb{Z}$, la classe de 2 est un diviseur de zéro, car $2 \times 2 \equiv 0 \ \ [4]$.

Exemple II.B.3. Dans l'anneau produit $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$, l'élément $(1, 0)$ est un diviseur de zéro, car :

$$(1, 0) \cdot (0, 1) = (0, 0).$$

Définition II.B.4. Un anneau A est dit *intègre* si $A \neq 0$ et A n'a pas de diviseurs de zéro, en d'autres termes,

$$\forall a, b \in A, \qquad ab = 0 \Longrightarrow (a = 0 \text{ ou } b = 0).$$

Exemple II.B.5. L'anneau $\mathbb{Z}$ est intègre. Les anneaux $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}^2$ ne le sont pas.

Exemple II.B.6. Tout corps $\mathbb{K}$ est intègre. En effet, si $a \in \mathbb{K} \setminus \{0\}$ était un diviseur de zéro, disons avec $b \in \mathbb{K} \setminus \{0\}$ tel que $ab = 0$, on aurait $aa^{-1} = 1$ et donc $b = baa^{-1} = 0$, une contradiction.

Proposition II.B.7. Soit A un anneau intègre. Si A est fini, alors c'est un corps.

Démonstration. Soit $a \in A$ un élément non nul. Considérons le morphisme de groupes (pour l'addition) $\varphi_a : A \to A, x \mapsto ax$. Comme A est intègre, cette application est injective : si $\varphi_a(x) = ax = 0$ alors $x = 0$. Comme source et but ont même cardinal fini, on en déduit qu'elle est également surjective. Il existe donc un élément $b \in A$ tel que $\varphi_a(b) = ab = 1$. ◇

Exemple II.B.8. Si A est un anneau intègre, tout sous-anneau de A est également intègre.

Exemple II.B.9. Si A est un anneau intègre, alors l'anneau des polynômes $A[X]$ aussi.

En règle générale, si $I \subset A$ est un idéal et que A est intègre, A/I n'est pas toujours intègre.

Définition II.B.10. Soit A un anneau et $I \subset A$ un idéal de A. On dit que I est un *idéal premier* si A/I est intègre ; ou en d'autres termes, si $I \neq A$ et :

$$\forall a, b \in A, \qquad ab \in I \Longrightarrow (a \in I \text{ ou } b \in I).$$

On note souvent les idéaux premiers « $\mathfrak{p}, \mathfrak{q}, \ldots$ ».

Exemple II.B.11. Soit n un entier. L'idéal $(n) \subset \mathbb{Z}$ est premier si et seulement si n est nul ou est un nombre premier (au signe près).

Exemple II.B.12. L'idéal engendré par $(0, 1)$ dans $\mathbb{Z}^2$ est premier, car le quotient est isomorphe à $\mathbb{Z} \times 0 \cong \mathbb{Z}$ qui est intègre.

Proposition II.B.13. Soit $f : A \to B$ un morphisme d'anneaux et $I \subset B$ un idéal premier. L'idéal $f^{-1}(I)$ est également premier.

Définition II.B.14. Soit A un anneau et $I \subset A$ un idéal. On dit que I est *maximal* si $I \neq A$ et si, quel que soit $J \subset A$ un idéal, si $I \subset J$, alors $J = I$ ou $J = A$.

En général, on note les idéaux maximaux « $\mathfrak{m}, \mathfrak{n}, \ldots$ ».

Proposition II.B.15. Soit A un anneau et I un idéal. Alors I est maximal si et seulement si A/I est un corps.

Démonstration. Supposons pour commencer que I est maximal. Alors $I \neq A$ donc A/I n'est pas l'anneau nul. Soit $[a] \in A/I$ une classe non nulle, avec $a \in A$, $a \notin I$. Soit $J = I + (a)$ la somme de I et de l'idéal engendré par (a). C'est un idéal qui contient *strictement* I, donc comme I est maximal, on a $J = A$. En particulier, $1 \in J$, donc il existe $x \in I$ et $b \in A$ tels que $x + ab = 1$. Dans l'idéal quotient, cela donne $[ab] = 1$, donc $[a]$ est inversible.

Réciproquement, supposons que A/I est un corps et montrons que I est maximal. Soit $I \subset J \subset A$ un idéal qui contient strictement I et soit $a \in J \setminus I$. La classe $[a] \in A/I$ est non-nulle, donc il existe une classe $[b] \in A/I$ telle que $[ab] = 1$, c'est-à-dire qu'il existe $x \in I$ tel que $ab + x = 1$. On a donc :

$$1 = ab + x \in (a) + I \subset J.$$

Or un idéal qui contient l'unité est l'anneau tout entier, donc $J = A$. ◇

Corollaire II.B.16. Un idéal maximal est premier.

Corollaire II.B.17. Un anneau A est un corps si et seulement s'il a exactement deux idéaux, $\{0\}$ et lui-même.

Exemple II.B.18. Soit n un entier. L'idéal $(n) \subset \mathbb{Z}$ est maximal si et seulement si n est un nombre premier (au signe près).

Exemple II.B.19. L'idéal $\big((0,1)\big) \subset \mathbb{Z}^2$ est premier mais pas maximal. Il est par exemple contenu dans l'idéal $\big((2,0),(0,1)\big)$ (qui est, lui, maximal).

Nous ne démontrerons pas le théorème suivant (qui nécessite l'axiome du choix).

Théorème II.B.20 (Krull). Soit I un idéal d'un anneau A. Si $I \neq A$, il existe un idéal maximal $\mathfrak{m} \subset A$ tel que $I \subset \mathfrak{m}$.

§ II.B(b) Anneaux factoriels

Aparté. La notion suivante est extrêmement importante en algèbre. Son histoire commence avec le dernier théorème de Fermat, qui cherche à déterminer si l'équation suivante admet des solutions entières avec $xyz \neq 0$, où $n \geq 2$ est entier :

$$x^n + y^n = z^n.$$

Elle en admet bien sûr pour $n = 2$: ce sont les triplets pythagoriciens, comme $2^2 + 3^2 = 5^2$ (les longueurs des côtés d'un triangle rectangle). Qu'en est-il pour $n \geq 3$? Fermat conjectura en 1637 qu'il n'existait aucune solution. Il prétendit avoir une preuve qui ne tenait pas dans la marge de son cahier. Il démontra quand même sa conjecture pour $n = 4$, ce qui entraîne aussi le résultat pour n non premier. Restent les cas où $n \geq 3$ est premier.

Des preuves ad-hoc furent trouvées pour $n \in \{3, 5, 7\}$, puis pour certaines classes de nombres premiers ; de nombreuses preuves fausses apparurent aussi au fil des siècles. Il fallut attendre la preuve de Wiles en 1994 pour enfin avoir une preuve correcte avec n quelconque : l'équation n'a aucune solution entière non-triviale pour $n \geq 3$.

Où se situait le problème dans les fausses preuves ? Si on pose $\zeta_p = \exp(2i\pi/p)$ une racine primitive $p$ième de l'unité, on peut réécrire l'équation comme :

$$z^p = \prod_{i=0}^{p-1} (x + \zeta_p^i y).$$

Si p ne divise pas xyz, alors les facteurs de ce produit sont premiers entre eux dans $\mathbb{Z}[\zeta_p]$. Si la décomposition de z^p en produit de facteurs dans $\mathbb{Z}[\zeta_p]$ est unique, alors cela entraîne que chaque $x + \zeta_p^i y$ est une puissance $p$ième dans l'anneau $\mathbb{Z}[\zeta_p]$. Avec la technique de descente infinie de Fermat, on en déduit une contradiction.

Le hic ? La décomposition en produit de facteurs de z^p n'est généralement pas unique ! L'anneau $\mathbb{Z}[\zeta_p]$ n'est en général pas *factoriel*. Il ne l'est pour aucun $p \geq 23$. La preuve ne fonctionne pas… Et on se rend compte que l'unicité de la décomposition en facteurs premiers, que l'on connaît bien dans $\mathbb{Z}$, n'est pas anodine !

Définition II.B.21. Soit A un anneau et $a, b \in A$ des éléments. On dit que a *divise* b, ou que b est un *multiple* de a, et on note $a \mid b$, s'il existe un élément $k \in A$ tel que $ak = b$.

Proposition II.B.22. Soit A un anneau et $a, b \in A$. Alors $a \mid b \Leftrightarrow (b) \subset (a)$.

Proposition II.B.23. La relation de divisibilité définit un préordre sur A (c.-à-d. elle est réflexive et transitive).

Définition II.B.24. Soit A un anneau et $a, b \in A$. On dit que a et b sont *associés* si les deux conditions $a|b$ et $b|a$ sont vérifiées (ce qui est équivalent à $(a) = (b)$).

Deux éléments associés sont essentiellement jumeaux du point de vue de l'arithmétique.

Exemple II.B.25. Des entiers $a, b \in \mathbb{Z}$ sont associés si et seulement si $a = \pm b$.

Proposition II.B.26. L'association définit une relation d'équivalence sur A. Si on note $\sim$ cette relation, l'ensemble quotient $A/\sim$ forme un ensemble ordonné pour la relation de divisibilité.

Proposition II.B.27. Soit A un anneau intègre. Des éléments $a, b \in A$ sont associés si et seulement s'il existe $u \in A^\times$ tel que $au = b$.

Démonstration. Il est clair que si u existe alors a et b sont associés (car $au = b$ et $bu^{-1} = a$). Réciproquement, supposons que a et b sont associés. Comme A est intègre, soit ils sont tous les deux nuls (auquel cas on prend $u = 1$), soit aucun des deux ne sont nuls. Plaçons-nous dans ce deuxième cas. Il existe $u, v \in A$ tels que $au = b$ et $bv = a$. On a donc $auv = bv = a$, donc $a(uv - 1)$. Comme $a \neq 0$, on a donc $uv = 1$, donc u et v sont inversibles. ◇

Exercice II.B.28. Soit $A = \mathbb{Z}[X, Y, Z]/\big(X(1 - YZ)\big)$. Montrer que X et XY sont associés mais qu'il n'existe pas d'élément inversible $u \in A^\times$ tel que $Xu = XY$.

Définition II.B.29. Soit A un anneau et $p \in A$. On dit que p est *irréductible* si $p \notin A^\times$ et si :

$$\forall a, b \in \mathrm{A}, \qquad p = ab \Longrightarrow (a \in A^\times \text{ ou } b \in A^\times).$$

Autrement dit, p n'est pas inversible et ses seuls diviseurs sont les unités et les associés de p.

Exemple II.B.30. Les entiers irréductibles sont les nombres premiers et leurs opposés.

Exemple II.B.31. Un corps ne contient pas d'élément irréductible.

Proposition II.B.32. Soit $p \in A \setminus \{0\}$ un élément non nul d'un anneau intègre. Si l'idéal (p) est premier, alors p est irréductible.

Démonstration. Supposons que (p) est premier. En particulier $(p) \neq A$ (car sinon $A/(p)$ serait l'anneau nul qui n'est pas intègre) donc $p \notin A^\times$. Supposons maintenant que $p = ab$ se décompose comme un produit. On a donc $ab \in (p)$, donc on a $a \in (p)$ ou $b \in (p)$. Quitte à échanger, supposons que $a = pc$ avec $c \in A$. On a alors $p = ab = pcb$ donc $p(1 - cb) = 0$. Comme $p \neq 0$ et que A est intègre, on a donc $cb = 1$, donc b est inversible. ◇

Remarque II.B.33. Le résultat de la proposition est faux en général si l'anneau n'est pas supposé intègre. Considérons par exemple $A = \mathbb{Z}^2$ et $p = (1, 0) \in \mathbb{Z}^2$. Alors l'idéal (p) est premier, mais p n'est pas irréductible, car on peut l'écrire comme un produit de facteurs qui ne sont pas inversibles :

$$p = (1, 0) \times (1, 2).$$

Exercice II.B.34. La réciproque est également fausse. Considérons l'anneau (intègre) suivant :

$$A = \mathbb{R}[X,Y]/(X^2 - Y^3).$$

Alors l'élément $[Y] \in A$ est irréductible et il divise le produit $[X] \cdot [X] = [X^2] = [Y^3] = [Y] \cdot [Y^2]$ mais il ne divise aucun des facteurs $[X]$ et $[X]$.

Définition II.B.35. Soit A un anneau et $a, b \in A$ des éléments. On dit que a et b sont *étrangers* si leurs seuls diviseurs communs sont les inversibles, c'est-à-dire :

$$\forall d \in A, \qquad (\, d \mid a \text{ et } d \mid b\,) \Longrightarrow d \in A^\times.$$

Exemple II.B.36. Deux entiers sont étrangers si et seulement s'ils sont premiers entre eux.

Définition II.B.37. Un anneau A est dit *factoriel* s'il est intègre et si tout élément non-nul est associé à un produit d'irréductibles, uniques à permutation et association près. En d'autres termes, quel que soit l'élément $a \in A \setminus \{0\}$,

- Il existe $u \in A^\times$ et $p_1, \dots, p_r$ irréductibles tels que $a = up_1 \dots p_r$;
- Si $a = vq_1 \dots q_s$ est une autre décomposition avec $v \in A^\times$ et les q_i irréductibles, alors $r = s$ et il existe une permutation $\sigma \in \mathfrak{S}_r$ telle que pour tout i, p_i est associé avec $q_{\sigma(i)}$.

Exemple II.B.38. L'anneau $\mathbb{Z}$ est factoriel.

Exemple II.B.39. Tout corps est (trivialement) factoriel : n'importe quel élément est associé à un produit vide d'irréductibles.

Exemple II.B.40. Soit $\mathbb{K}$ un corps. L'anneau $\mathbb{K}[X]$ est factoriel. Pour le démontrer, il faut quelques outils supplémentaires que l'on verra dans les sections suivantes.

Exercice II.B.41. L'anneau $\mathbb{Z}[i\sqrt{5}] = \{x + iy\sqrt{5} \mid x, y \in \mathbb{Z}\}$ n'est pas factoriel. Il est bien intègre (c'est un sous-anneau de $\mathbb{C}$ qui est un corps), mais on a la décomposition suivante :

$$6 = 2 \times 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}).$$

On vérifiera que 2, 3, $1 + i\sqrt{5}$ et $1 - i\sqrt{5}$ sont irréductibles mais ne sont pas associés deux à deux.

Exemple II.B.42. L'anneau des fonctions holomorphes sur $\mathbb{C}$ est intègre mais n'est pas factoriel. Par exemple, la fonction sinus est divisible par chacune des fonctions $z \mapsto z - k\pi$ (pour $k \in \mathbb{Z}$), qui sont toutes irréductibles et qui ne sont pas associées deux à deux ; donc une décomposition de la fonction sinus aurait une infinité de facteurs irréductibles.

Il est assez fréquent qu'un anneau vérifie la condition d'existence dans la définition d'anneau factoriel ; c'est la condition d'unicité qui est forte. Vérifier cette condition d'unicité peut s'avérer difficile. Le critère suivant permet de simplifier cela.

Proposition II.B.43. Soit A un anneau intègre tel que tout élément non nul est associé à un produit d'irréductibles. Les propositions suivantes sont équivalentes :

(a) L'anneau A est factoriel.
(b) (Lemme d'Euclide) Si $p \in A$ est irréductible, et si p divise ab, alors il divise a ou il divise b.
(c) (Réciproque de **Proposition II.B.32**) Si $p \in A$ est irréductible alors l'idéal (p) est premier.
(d) (Lemme de Gauss) Si a divise bc et si a et b sont étrangers, alors a divise c.

Démonstration. L'équivalence entre « (b) ⟺ (c) » est évidente, simplement en réécrivant la définition. L'implication « (d) ⟹ (b) » est également évidente.

Démontrons que (b) implique (a). Supposons que l'on puisse décomposer un élément de A de deux manières différentes, où $u, v \in A^\times$ et p_i, q_j irréductibles :

$$up_1 \dots p_k = vq_1 \dots q_l.$$

Alors p_1 divise $q_1 \dots q_l$, donc il divise l'un des q_j. Mais comme q_j est irréductible, p_1 et q_j sont associés. En continuant ainsi par récurrence, on en déduit que les deux écritures sont égales à permutation et association près.

Démontrons enfin que (a) entraîne (d). Soit a, b, c des éléments tels que $a \mid bc$ et tels que a et b soient étrangers. Soient $p_1, \dots, p_n$ tous les irréductibles qui apparaissent dans les décompositions de a, b et c. On peut ainsi écrire, où $\alpha_i, \beta_i, \gamma_i \in \mathbb{N}$ et $u, v, w \in A^\times$:

$$a = u\prod_{i=1}^{n} p_i^{\alpha_i}, \qquad b = v\prod_{i=1}^{n} p_i^{\beta_i}, \qquad c = w\prod_{i=1}^{n} p_i^{\gamma_i}.$$

Par hypothèse, $a \mid bc$ donc pour tout i, on a $\alpha_i \leq \beta_i + \gamma_i$. Pour chaque i, il y a deux possibilités :

> Si $\alpha_i = 0$, alors bien sûr $\alpha_i \leq \gamma_i$.
> Si $\alpha_i > 0$, alors on doit avoir $\beta_i = 0$, car sinon, a et b ne seraient pas étrangers (ils seraient tous deux divisibles par p_i). On a donc également $\alpha_i \leq \gamma_i$.

Donc pour tout i, on a $\alpha_i \leq \gamma_i$; en d'autres termes, a divise c. ◇

Notons $A/\sim$ le quotient de A par la relation d'association, comme dans la **Proposition II.B.26**. On rappelle que cet ensemble est ordonné par la relation de divisibilité.

Proposition II.B.44. Soit A un anneau factoriel. L'ensemble $A/\sim$ est *réticulé* (on dit également que c'est un treillis), c'est-à-dire qu'étant données des classes $a, b \in A/\sim$, l'ensemble $\{a, b\}$ possède une borne supérieure et une borne inférieure.

Démonstration. Soit $a = u\prod_{i=1}^{n} p_i^{\alpha_i}$ et $b = v\prod_{i=1}^{n} p_i^{\beta_i}$ les décompositions de a et b en produits d'irréductibles, alors $\alpha_i, \beta_i \in \mathbb{N}$ (on s'autorise des puissances nulles pour avoir la même liste dans a et b). Il est aisé de vérifier que la borne supérieure de $\{a, b\}$ est donnée par la classe de $\prod_{i=1}^{n} p_i^{\max(\alpha_i,\beta_i)}$ et que la borne inférieure est donnée par la classe de $\prod_{i=1}^{n} p_i^{\min(\alpha_i,\beta_i)}$. ◇

Définition II.B.45. Soit A un anneau factoriel et $a, b \in A$ des éléments. Le *PGCD* (resp., le *PPCM*) de a et b, noté $a \wedge b$ (resp., $a \vee b$), est la classe de la borne inférieure (resp., supérieure) de $\{a, b\}$ dans l'ensemble ordonné $A/\sim$.

Remarque II.B.46. Le PGCD et le PPCM ne sont définis qu'à association près. Les idéaux engendrés par le PGCD et par le PPCM sont, eux, bien définis (car $a \sim b \Leftrightarrow (a) = (b)$).

Proposition II.B.47. Soit A un anneau factoriel et $a, b \in A$. On a $(a \vee b) = (a) \cap (b)$.

Démonstration. Comme $a \mid a \vee b$ et $b \mid a \vee b$, on a bien $(a \vee b) \subset (a)$ et $(a \vee b) \subset (b)$ d'où $(a \vee b) \subset (a) \cap (b)$. Réciproquement, soit $c \in (a) \cap (b)$. Alors $a \mid c$ et $b \mid c$, donc par définition du PPCM, $a \vee b \mid c$ et donc $c \in (a \vee b)$. ◇

Remarque II.B.48. Bien qu'on ait toujours $(a) + (b) \subset (a \wedge b)$, on n'a en général pas l'égalité. Prenons $A = \mathbb{R}[X, Y]$. Alors le PGCD des polynômes X et Y est $X \wedge Y = 1$ (car si un polynôme P divise à la fois X et Y alors il est constant). Mais on n'a pas $(X) + (Y) = (1)$, car on ne peut pas écrire $1 = XP + YQ$ avec $P, Q \in \mathbb{R}[X, Y]$.

§ II.B(c) Anneaux principaux

Pour pallier le problème de la **Remarque II.B.48**, introduisons la notion d'anneau principal. Dans ces anneaux, l'arithmétique est bien plus simple !

Définition II.B.49. Soit A un anneau et $I \subset A$ un idéal. On dit que I est un *idéal principal* s'il existe un élément $a \in A$ tel que $I = (a)$.

Définition II.B.50. Un *anneau principal* est un anneau intègre dont tous les idéaux sont principaux.

Exemple II.B.51. Tout corps est un anneau principal.

Exemple II.B.52. L'anneau $\mathbb{Z}$ est principal. La démonstration attendra le § II.B(e).

Exemple II.B.53. Si $\mathbb{K}$ est un corps, alors $\mathbb{K}[X]$ est principal. La démonstration attendra le § II.B(e).

Exercice II.B.54. L'anneau $\mathbb{Z}[X]$ n'est pas principal, car l'idéal $(2, X)$ n'est pas principal.

On admettra le résultat suivant. La démonstration utilise la notion d'anneau noethérien (voir § II.B(d)) qui n'est pas au programme du cours.

Proposition II.B.55 (admis, voir Corollaire II.B.75). Un anneau principal est factoriel.

En particulier, on peut définir le PGCD et le PPCM dans un anneau principal. On a vu que le PPCM est caractérisé par l'identité $(a) \cap (b) = (a \vee b)$. La proposition suivante donne une caractérisation similaire du PGCD dans un anneau principal :

Proposition II.B.56 (Identité de Bézout). Soit A un anneau principal et $a, b \in A$. On a l'égalité :

$$(a) + (b) = (a \wedge b).$$

Démonstration. Nous savons déjà que $(a) + (b) \subset (a \wedge b)$: c'est vrai dans n'importe quel anneau factoriel. Comme A est principal, l'idéal $(a) + (b)$ est engendré par un élément, disons $c \in A$. Comme $a \in (a) \subset (c)$, on a $c \mid a$. De même, on a $c \mid b$. Donc c est un diviseur commun à a et b, donc $c \mid a \wedge b$, ce qui revient à $(a \wedge b) \subset (c) = (a) + (b)$. ◇

Corollaire II.B.57 (Théorème de Bézout). Soit A un anneau principal et $a, b \in A \setminus \{0\}$ deux éléments étrangers. Il existe $x, y \in A$ tels que $ax + by = 1$.

Démonstration. Si a et b sont étrangers, leurs seuls diviseurs communs sont inversibles, donc $a \wedge b = 1$. Grâce à la proposition suivante, on a $A = (1) = (a) + (b)$, ce qui permet de conclure. ◇

Concluons par la description suivante des idéaux premiers d'un anneau principal. La démonstration est claire en utilisant les outils déjà introduits.

Proposition II.B.58. Soit A un anneau principal qui n'est pas un corps. Ses idéaux premiers sont (0) et les idéaux de la forme (p) avec p irréductible ; ces derniers sont maximaux.

Corollaire II.B.59. Le quotient d'un anneau principal par un idéal premier est encore principal.

Démonstration. En effet, si $\mathfrak{p} \subset A$ est premier, alors soit $\mathfrak{p} = 0$ auquel cas $A/0 = A$ est principal ; soit $\mathfrak{p} = (p)$ est engendré par un élément irréductible et est maximal, auquel cas $A/\mathfrak{p}$ est un corps, donc principal. ◇

Remarque II.B.60. Si $I \subset A$ n'est pas premier, alors A/I ne peut de toute manière pas être principal, car un anneau principal est intègre par définition.

Exercice II.B.61. Soit A un anneau factoriel tel que tout idéal premier non nul est maximal.

- Montrer que si $a, b \in A \setminus \{0\}$, il existe $x, y \in A$ tels que $ax + by = a \wedge b$.
- Soit $I \subset A$ un idéal non nul. Montrer qu'il existe $d \in A$ qui est le PGCD de tous les éléments de $I \cap (A \setminus \{0\})$.
- En déduire que A est principal.

§ II.B(d) Anneaux noethériens ☆

Les anneaux principaux sont finalement assez rares. Introduisons maintenant une généralisation, les anneaux noethériens. Cette classe d'anneaux, fondamentale en algèbre, vérifie une propriété de finitude remarquablement stable par les opérations usuelles sur les anneaux.

Définition II.B.62. Soit A un anneau et I un idéal. On dit que I est de *type fini* s'il est engendré par un nombre fini d'éléments, c'est-à-dire s'il existe $a_1, \dots, a_r \in I$ tels que :

$$I = (a_1, \dots, a_r).$$

Définition II.B.63. Un anneau A est dit *noethérien* si tous ses idéaux sont de type fini.

Exemple II.B.64. Les anneaux principaux sont noethériens : chaque idéal est engendré par un élément.

Proposition II.B.65. Soit A un anneau. Les propositions suivantes sont équivalentes :

(a) L'anneau A est noethérien.
(b) Toute suite croissante $I_0 \subset I_1 \subset \cdots \subset I_n \subset \cdots$ d'idéaux de A est stationnaire, c'est-à-dire :
$$\exists n_0 \in \mathbb{N}, \qquad \forall n \geq n_0, \qquad I_n = I_{n_0}.$$
(c) Un ensemble non vide d'idéaux de A admet un élément maximal pour l'inclusion.

Démonstration. Commençons par démontrer (a) ⇒ (b). Soit $I_0 \subset I_1 \subset \cdots$ une suite croissante d'idéaux. La réunion de ces idéaux forme un nouvel idéal (petit exercice) :

$$I_\infty = \bigcup_{n=0}^{\infty} I_n.$$

Comme A est noethérien, il existe des éléments $a_1, \dots, a_r \in I$ qui engendrent I_∞. Chacun de ces éléments est dans l'un des I_n ; notons n_0 le plus grand des indices, de telle sorte que $a_1, \dots, a_r \in I_{n_0}$. Alors pour tout $n \geq n_0$, on a $I_n \subset I_\infty = (a_1, \dots, a_n) = I_{n_0}$ et la suite est stationnaire.

Démontrons maintenant que (b) entraîne (c). Soit E un ensemble non vide d'idéaux de A. Supposons (par l'absurde) que E n'a pas d'élément maximal. On construit une suite par récurrence qui contredit l'hypothèse (b) : on choisit un idéal $I_0 \in E$ quelconque ; comme il n'est pas maximal, on peut trouver $I_1 \in E$ tel que $I_0 \subsetneq I_1$; ainsi de suite, on construit une suite d'idéaux qui n'est pas stationnaire.

Enfin, démontrons que (c) implique (a). Soit I un idéal quelconque de A. On note E l'ensemble des sous-idéaux de I qui sont de type fini. Cet ensemble n'est pas vide (il contient par exemple (0)), donc par hypothèse, il admet un élément maximal, disons $J = (a_1, \dots, a_r) \subset I$. Supposons que $I \neq J$ et choisissons $b \in I \setminus J$; on aurait alors $J \subsetneq (a_1, \dots, a_r, b) \subset I$, ce qui contredirait la maximalité de J, donc $I = J$. L'idéal $I = J \in E$ est donc bien de type fini. ◇

Corollaire II.B.66. Un quotient d'un anneau noethérien est noethérien.

Démonstration. Cela découle directement de la caractérisation précédente et du fait que les idéaux de A/I sont les idéaux de A contenant I. Une suite croissante d'idéaux de A/I est une suite d'idéaux de A (contenant I), donc elle est stationnaire. ◇

Exercice II.B.67. Un sous-anneau d'un anneau noethérien n'est pas toujours noethérien. L'anneau $\mathbb{R}[X,Y]$ est noethérien, mais le sous-anneau engendré par $\{X, XY, XY^2, \dots\}$ ne l'est pas.

Théorème II.B.68 (Hilbert). Soit A un anneau noethérien. L'anneau $A[X]$ est aussi noethérien.

Définition II.B.69. Pour un idéal $I \subset A$ et un entier $n \geq 0$, on définit l'idéal suivant :

$$d_n(I) \coloneqq \{\text{coefficients dominants des éléments de } I \text{ de degré } n\} \cup \{0\} \subset A.$$

Lemme II.B.70. Les fonctions d_n vérifient les propriétés suivantes :

- Quel que soient I et n, $d_n(I) \subset d_{n+1}(I)$.
- Si $I \subset J$ sont deux idéaux imbriqués, alors $d_n(I) \subset d_n(J)$ pour tout n. De plus, $I = J$ si et seulement si $\forall n \geq 0,\ d_n(I) = d_n(J)$.

Démonstration. Pour tout n, $d_n(I) \subset d_{n+1}(I)$ (car si $P \in A[X]$ est de degré n, son coefficient dominant est le coefficient dominant de XP qui est de degré $n+1$).

Enfin, étant donné des idéaux $I \subset J$, montrons que $I = J$ si et seulement si $\forall n \geq 0,\ d_n(I) = d_n(J)$. L'implication directe est évidente. Si au contraire $I \neq J$, choisissons $P \in J \setminus I$ de degré minimal, disons $k = \deg(P)$. S'il existait $Q \in I$ de même degré k et de même coefficient dominant que P, alors on aurait $\deg(P-Q) < k$ et $P - Q \in J \setminus I$, ce qui contredit la minimalité du degré de P. On doit donc avoir $d_k(I) \neq d_k(J)$. ◇

Démonstration du théorème d'Hilbert. Supposons que l'on ait une suite croissante d'idéaux de $A[X]$:

$$I_0 \subset I_1 \subset \cdots \subset I_n \subset \cdots$$

Nous cherchons à montrer que cette suite est stationnaire. Comme A est noethérien, l'ensemble suivant d'idéaux de A possède un élément maximal :

$$E = \{\, d_k(I_n) \mid k, n \geq 0 \,\}.$$

Supposons que $d_{k_0}(I_{n_0})$ soit maximal. Étant donné $k \leq k_0$, la suite $d_k(I_0) \subset d_k(I_1) \subset \cdots$ est une suite croissante d'idéaux de A, donc elle stationne à partir d'un indice m_k, c'est-à-dire $\forall n \geq m_k,\ d_k(I_n) = d_k(I_{m_k})$. Posons l'entier :

$$N \coloneqq \max(n_0, m_0, \dots, m_{k_0}).$$

Nous allons montrer que la suite $\{I_n\}$ stationne en I_N. D'après le lemme précédent, il suffit de montrer que pour tout k et tout $n \geq N$, on a $d_k(I_n) = d_k(I_N)$. Il y a deux cas possibles :

- Si $k \geq k_0$, alors on a $d_{k_0}(I_{n_0}) \subset d_k(I_{n_0}) \subset d_k(I_n)$. Comme $d_{k_0}(I_{n_0})$ est maximal dans E, on a $d_k(I_n) = d_{k_0}(I_{n_0})$. De la même manière, $d_{k_0}(I_{n_0}) \subset d_k(I_{n_0}) \subset d_k(I_N)$ donc on a aussi $d_k(I_N) = d_{k_0}(I_{n_0})$ et finalement on a bien $d_k(I_n) = d_k(I_N)$.
- Si au contraire $k < k_0$, la suite $d_k(I_\cdot)$ stationne en $d_k(I_{m_k})$. Comme $n \geq N \geq m_k$, on a donc bien $d_k(I_n) = d_k(I_N)$.

La suite $\{I_n\}$ est donc bien stationnaire en N. ◇

Corollaire II.B.71. Si A est noethérien, alors tous les anneaux $A[X_1, \dots, X_n]$ le sont aussi.

Corollaire II.B.72. Soit A un anneau noethérien. Toute A-algèbre de type fini est noethérienne.

Remarque II.B.73. Il existe des algèbres noethériennes qui ne sont pas de type fini. Par exemple, étant donné un corps $\mathbb{K}$, l'anneau $\mathbb{K}[\![X]\!]$ des séries formelles est noethérien mais n'est pas une $\mathbb{K}$-algèbre de type fini.

Proposition II.B.74. Soit A un anneau intègre noethérien. Tout élément de A est associé à un produit d'irréductibles.

Démonstration. On considère le sous-ensemble suivant des idéaux de A :

$$E = \{ (a) \mid a \neq 0 \text{ ne s'écrit pas sous la forme } up_1 \dots p_r \}.$$

Supposons que E et non vide. Il admet donc un élément maximal, disons (a). L'élément a n'est ni inversible, ni irréductible, donc il existe une décomposition $a = bc$ avec $b, c \notin A^\times$. On a en particulier $(a) \subsetneq (b)$ et $(a) \subsetneq (c)$. Comme (a) est maximal dans E, on a donc $(b) \notin E$ et $(c) \notin E$, donc on peut écrire $b = up_1 \dots p_r$ et $c = q_1 \dots q_s$. Mais alors on a $a = uvp_1 \dots p_r q_1 \dots q_s$, ce qui contredit $(a) \in E$. ◇

Corollaire II.B.75. Un anneau principal est factoriel.

Démonstration. Soit A un anneau principal. Tout anneau principal est intègre. De plus, A est noethérien, donc tout élément de A est associé à un produit d'irréductible par la proposition précédente. Grâce au critère de la **Proposition II.B.43**, il suffit de démontrer que si p est irréductible alors (p) est premier. Or être irréductible revient à être maximal parmi les idéaux principaux distincts de A. Comme A est principal, c'est que (p) est donc maximal tout court, et un idéal maximal est premier. ◇

Remarque II.B.76. Il existe une notion « duale » à la notion d'anneau noethérien, les anneaux artiniens, pour lesquels on demande tout suite décroissante d'idéaux d'être stationnaire. Cette condition est plus forte que celle d'être noethérien : tout anneau artinien est également noethérien.

§ II.B(e) Anneaux euclidiens

Terminons cette liste de propriétés par une nouvelle qui s'avère bien utile pour démontrer qu'un anneau est principal.

Définition II.B.77. Un *anneau euclidien* est un anneau $A \neq 0$ muni d'une fonction[7] $\nu : A \setminus \{0\} \to \mathbb{N}$ telle que :

- Si $a \in A$ et $b \in A \setminus \{0\}$, il existe $q, r \in A$ tels que :
$$a = bq + r \quad \text{et} \quad \big(r = 0 \text{ ou } \nu(r) < \nu(b)\big).$$
- Pour tous $a, b \in A \setminus \{0\}$, si a divise b alors $\nu(a) \leq \nu(b)$.

Exemple II.B.78. L'anneau $\mathbb{Z}$ muni de la fonction $\nu(n) = |n|$ est euclidien.

Exercice II.B.79. L'anneau $\mathbb{Z}[i]$ des entiers de Gauss, muni de la fonction $\nu(z) = z\bar{z}$, est euclidien.

Remarque II.B.80. On peut simplifier la première condition de la définition en posant $\nu(0) = -\infty$. Alors pour $a, b \in A$, $b \neq 0$, il existe $q, r \in A$ tels que $a = bq + r$ et $\nu(r) < \nu(b)$.

[7] Cette fonction est parfois appelée « stathme ».

Remarque II.B.81. Les éléments q et r de la définition ne sont pas nécessairement uniques. Par exemple, dans $\mathbb{Z}$, avec $a = 10$ et $b = 3$, on a :

$$a = 3b + 1 = 4b + (-2).$$

Proposition II.B.82. Soit A un anneau euclidien. Il existe une constante $\nu_0 \in \mathbb{N}$ telle que pour tout $x \in A^\times$ inversible, $\nu(x) = \nu_0$. De plus, étant donné $a \in A \setminus \{0\}$ quelconque, on a $\nu(a) \geq \nu_0$ et l'égalité est atteinte si et seulement si a est inversible.

Démonstration. Soient x et y des éléments inversibles quelconques. On a $\nu(x) \leq \nu(xx^{-1}y) = \nu(y) \leq \nu(yy^{-1}x) = \nu(x)$ donc $\nu(x) = \nu(y)$.

Si $a \in A \setminus \{0\}$ est quelconque et $x \in A^\times$ est inversible, x divise $a = xx^{-1}a$, donc $\nu_0 = \nu(x) \leq \nu(a)$. Enfin, supposons que $\nu(a) = \nu_0$. En effectuant la division euclidienne de 1 par a, on trouve des éléments $q, r \in A$ tels que :

$$1 = aq + r, \qquad \nu(r) < \nu(a).$$

On a donc $\nu(r) < \nu(a) = \nu_0$. Or, d'après ce que l'on vient de démontrer, si r était non nul, on aura $\nu(r) \geq \nu_0$; c'est donc que $r = 0$. Donc on a $1 = aq$ et $a \in A^\times$. ◇

Remarque II.B.83. On peut toujours renormaliser l'anneau euclidien de telle sorte que $\nu_0 = 1$ en remplaçant $\nu(\_)$ par $\nu(\_) - \nu_0 + 1$.

Théorème II.B.84. Tout anneau euclidien est principal.

Démonstration. Soit $I \subset A$ un idéal d'un anneau euclidien. On peut supposer $I \neq 0$ (car 0 est évidemment principal). L'ensemble $\{\nu(x) \mid x \in I\} \subset \mathbb{N}$ est un sous-ensemble non vide des entiers naturels, et il admet donc un minimum, disons $n_0 = \nu(x_0)$ avec $x_0 \in I$.

Démontrons que $I = (x_0)$. Soit $y \in I$ un élément de I. Comme A est euclidien, il existe des éléments $q, r \in A$ tels que $y = qx_0 + r$ et soit $r = 0$, soit $\nu(r) < \nu(x_0)$. Mais on a $r = y - qx_0 \in I$, donc si r était non nul, on aurait $\nu(r) < \nu(x_0)$, ce qui contredit le fait que $\nu(x_0)$ est minimal. C'est donc que $r = 0$ et on a donc $y = qx_0$, ou encore $x_0 \mid y$. ◇

Corollaire II.B.85. Les anneaux $\mathbb{Z}$ et $\mathbb{Z}[i]$ sont principaux.

Exercice II.B.86. Soit $\xi = \frac{1}{2}\left(1 + i\sqrt{19}\right)$. L'anneau $\mathbb{Z}[\xi]$ est principal mais pas euclidien.

L'exercice précédent montre qu'un quotient d'un anneau euclidien n'est pas nécessairement euclidien lui-même.

Section II.C. Corps des fractions

On sait bien que l'anneau $\mathbb{Z}$ n'est pas un corps : l'élément $2 \in \mathbb{Z}$ n'est pas inversible, par exemple. On sait aussi comment résoudre cette difficulté de la manière la plus « efficace » possible, en construisant le corps des nombres rationnels $\mathbb{Q}$. Ce corps est, en quelque sorte, le « plus petit corps » qui contient $\mathbb{Z}$. Nous allons maintenant généraliser cette construction.

Définition II.C.1. Soit A un anneau intègre. On définit le *corps des fractions* de A, noté K_A (ou parfois $\mathrm{Frac}(A)$) de la façon suivante.

- L'ensemble $A \times (A \setminus \{0\})$ est muni d'une relation d'équivalence définie par :
$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

L'ensemble K_A est le quotient de $A \times (A \setminus \{0\})$ par cette relation d'équivalence.

- L'addition sur K_A est définie par :
$$(a, b) + (c, d) = (ad + bc, bd).$$
L'élément neutre pour l'addition est la classe de $(0, 1)$.
- La multiplication sur K_A est définie par :
$$(a, b) \times (c, d) = (ac, bd).$$
L'élément neutre pour la multiplication est la classe de $(1, 1)$.

Proposition II.C.2. La définition précédente définit un corps K_A : la relation indiquée est bien une relation d'équivalence, l'addition donnée est bien définie, associative, commutative et unitaire, la multiplication est bien définie, associative, commutative, unitaire, et distributive par rapport à l'addition, et tout élément non nul est inversible.

Démonstration. La preuve ne pose pas de difficultés particulières. Le seul point un tant soit peu subtil est la transitivité de la relation d'équivalence. En effet, supposons que $(a, b) \sim (c, d)$ et $(c, d) \sim (e, f)$. En d'autres termes, on a $ad = bc$ et $cf = de$. On obtient donc $acf = ade = bce$. Si $c \neq 0$, cela permet bien de conclure que $af = be$ (et donc $(a, b) \sim (e, f)$) car A est intègre. Si au contraire $c = 0$, alors $ad = de = 0$. Or d est inversible, et A est toujours intègre, donc $a = e = 0$ et donc on a bien $(a, b) \sim (e, f)$. ◇

Tombons les masques : étant donné un anneau intègre A et des éléments $(a, b) \in A \times (A \setminus \{0\})$, nous allons noter a/b ou $\frac{a}{b}$ la classe de (a, b) dans K_A. Les définitions de la relation d'équivalence, de l'addition et de la multiplication paraissent sans doute plus naturelles avec cette écriture.

La proposition suivante est évidente :

Proposition II.C.3. Il existe un morphisme d'anneaux canonique injectif :
$$\iota : A \to K_A, \qquad a \mapsto \frac{a}{1}.$$

La proposition suivante dit que K_A est le « corps universel[8] » construit à partir de A.

Proposition II.C.4. Soit A un anneau intègre, $\mathbb{K}$ un corps et $f : A \to \mathbb{K}$ un morphisme d'anneaux injectifs. Il existe un unique morphisme de corps $\bar{f} : K_A \to \mathbb{K}$ tel que $\bar{f} \circ \iota = f$.

Démonstration. Soit $a/b \in K_A$ une fraction. Comme $b \neq 0$, on a $f(b) \neq 0$ (f est injectif) et possède donc un inverse dans $\mathbb{K}$. On peut donc définir $\bar{f}(a/b) \coloneqq f(a)\, f(b)^{-1}$ et il est aisé de vérifier que $\bar{f}$ ainsi défini est un morphisme de corps qui étend f.

Supposons maintenant que $g : K_A \to \mathbb{K}$ est un (autre) morphisme qui étend f, c'est-à-dire $g(a/1) = f(a)$ pour tout a. Alors pour $b \in A \setminus \{0\}$, on a $g(b/1)g(1/b) = g(b/b) = g(1/1) = 1$, donc $g(1/b)$ est l'inverse multiplicatif de $g(b/1) = f(b)$. On obtient donc :
$$g\left(\frac{a}{b}\right) = g\left(\frac{a}{1} \cdot \frac{1}{b}\right) = g\left(\frac{a}{1}\right) \cdot g\left(\frac{1}{b}\right) = f(a) \cdot f(b)^{-1} = \bar{f}\left(\frac{a}{b}\right).$$ ◇

Exemple II.C.5. Le corps des fractions de $\mathbb{Z}$ est $\mathbb{Q}$.

[8] Les aficionados de la théorie des catégories pourront interpréter ce résultat comme une adjonction de foncteurs.

Exemple II.C.6. Le corps des fractions de $\mathbb{K}[X]$ (où $\mathbb{K}$ est un corps) est le corps des fractions rationnelles en une variable, généralement noté $\mathbb{K}(X)$.

Exercice II.C.7. Le corps des fractions de l'anneau des entiers de Gauss $\mathbb{Z}[i]$ est l'anneau des fractions de Gauss, $\mathbb{Q}[i] = \{ a + bi \mid a, b \in \mathbb{Q} \}$.

Remarque II.C.8. Il existe une notion plus générale (que nous n'utiliserons pas dans ce cours), la notion de localisation, qui consiste à inverser une partie des éléments de l'anneau. On peut voir K_A comme la localisation de A par rapport à $A \setminus \{0\}$.

Section II.D. Anneaux de polynômes

Dans cette section, nous allons étudier plus en détail les anneaux de polynômes de la forme $A[X_1, \dots, X_n]$, introduits dans la Section II.A, qui sont fondamentaux en algèbre.

Lemme II.D.1. Soit A un anneau intègre. Si $P, Q \in A[X] \setminus \{0\}$ sont des polynômes non nuls, alors $\deg(PQ) = \deg(P) + \deg(Q)$.

Démonstration. On peut écrire $P = \sum_{i=0}^{m} a_i X^i$ et $Q = \sum_{i=0}^{n} b_i X^i$ avec $m = \deg(P)$, $n = \deg(Q)$, $a_m \neq 0$ et $b_n \neq 0$. On a alors :

$$PQ = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j \right) X^i.$$

En particulier, le coefficient de X^{m+n} est $a_m b_n$, qui est non nul car A est intègre. Donc $\deg(PQ) = m + n$ est bien égal à $\deg(P) + \deg(Q)$. ◇

Remarque II.D.2. Le résultat est faux si A n'est pas intègre. Prenons par exemple $A = \mathbb{Z}/4\mathbb{Z}$ et $P = Q = 2X + 1$. Alors $\deg(P) = \deg(Q) = 1$, mais $PQ = (2X + 1)^2 = 1 \pmod 4$ donc $\deg(PQ) = 0 \neq 2$.

Proposition II.D.3. Soit A un anneau. L'anneau $A[X]$ est intègre si et seulement si A l'est.

Si $A[X]$ est intègre, son sous-anneau A l'est aussi. Le lemme précédent implique la réciproque. ◇

Déterminons maintenant quand $A[X]$ est principal. Nous aurons besoin de quelques lemmes pour commencer.

Lemme II.D.4. Soit A un anneau et soit $P \in A[X]$ un polynôme non nul de coefficient dominant inversible. Pour tout $F \in A[X]$, il existe des polynômes $Q, R \in A[X]$ tels que :

$$F = PQ + R \quad \text{et} \quad (R = 0 \text{ ou } \deg(R) < \deg(P)).$$

Démonstration. Quitte à diviser l'équation par le coefficient dominant de P, on peut supposer que P est unitaire :

$$P = X^d + a_{d-1} X^{d-1} + \cdots + a_1 X + a_0.$$

Le problème revient au suivant : étant donné l'anneau $B = A[X]/(P)$, il s'agit de montrer que tout élément $[F] \in B$ est égal (modulo P) à une combinaison linéaire de $[X^0], \dots, [X^{d-1}]$. Comme ce problème est linéaire, il suffit de le résoudre pour les monômes et on peut supposer que $F = X^n$.

Le résultat voulu est évident si $n < d$. Supposons que le résultat est vrai pour tous les $n < n_0$ avec $n_0 \geq d$ fixé et montrons qu'il est vrai pour $n = n_0$. On a la relation suivante dans B :

$$[X^{n_0}] = [X^{n_0-d}][X^d] = [X^{n_0-d}](-a_{d-1}[X^{d-1}] - \cdots - a_1[X] - a_0)$$
$$= -a_{d-1}[X^{n_0-1}] - \cdots - a_1[X^{n_0-d-1}] - a_0[X^{n_0-d}].$$

On peut appliquer l'hypothèse de récurrence : chacun des termes $[X^{n_0-1}], \dots, [X^{n_0-d}]$ est égal à une combinaison linéaire de $[X^0], \dots, [X^{d-1}]$, donc $[X^{n_0}]$ aussi. ◇

Corollaire II.D.5. Soit $\mathbb{K}$ un corps. L'anneau $\mathbb{K}[X]$ est euclidien, donc principal.

Il suffit de prendre $v(P) = \deg(P)$. Tous les polynômes non nuls de $\mathbb{K}[X]$ ont un coefficient dominant inversible, donc on peut appliquer le lemme précédent. ◇

Proposition II.D.6. Soit A un anneau. Si $A[X]$ est principal, alors A est un corps.

Supposons que $A[X]$ est principal. Il est en particulier intègre, donc son sous-anneau A aussi. L'élément $X \in A[X]$ est irréductible. En effet, si on écrit $X = PQ$, l'un des deux termes P ou Q est constant et l'autre de degré 1 grâce au **Lemme II.D.1**. Quitte à échanger, écrivons $P = aX$ et $Q = b$ où $a, b \in A$. On a $X = PQ = abX$ d'où $ab = 1$ et a et b sont inversibles ; en particulier, $Q = b$ est inversible.

Comme $A[X]$ est supposé principal, l'idéal (X) engendré par l'élément irréductible X est maximal. Or, $A[X]/(X) = A$, donc A est un corps. ◇

En particulier, si A est un anneau principal quelconque, $A[X]$ n'est en général pas principal.

Exemple II.D.7. L'anneau $\mathbb{Z}[X]$ n'est pas principal car l'idéal $(2, X)$ ne l'est pas.

La factorialité est conservée par le passage à l'anneau des polynômes. Encore un théorème de Gauss !

Théorème II.D.8 (Gauss). Si un anneau A est factoriel, alors l'anneau $A[X]$ l'est aussi.

À partir de maintenant, on fixe l'anneau factoriel A. Notons déjà que $A[X]$ est intègre et que $A[X]^\times = A^\times$ pour des raisons de degré. La démonstration utilise la notion suivante.

Définition II.D.9. Soit $P \in A[X]$ un polynôme non nul. Le *contenu* de P, noté $c(P)$, est le PGCD des coefficients de P. Dit autrement, si on écrit $P = a_0 + a_1X + \cdots + a_nX^n$, alors :

$$\mathrm{c}(P) = \mathrm{pgcd}(a_0, \dots, a_n) \in A/A^\times.$$

Un polynôme P est *primitif* si $\mathrm{c}(P) = 1$.

Remarque II.D.10. Un polynôme P est primitif si ses coefficients sont (globalement) premiers entre eux. Notons que cela n'est pas la même chose qu'être premiers entre eux deux à eux ! Si par exemple $P = X^2 + 2X + 2 \in \mathbb{Z}[X]$, alors $\mathrm{c}(P) = 1$ (car $\mathrm{pgcd}(1, 2, 2) = 1$) mais les coefficients de P ne sont pas premiers entre eux deux à deux.

Remarque II.D.11. Si $P \in A[X]$ alors $\mathrm{c}(P)$ divise P et on peut écrire $P = c(P)\,\tilde{P}$ où $\tilde{P}$ est primitif.

Lemme II.D.12 (Gauss). Soit P et Q deux polynômes non nuls à coefficients dans A, on a :

$$\mathrm{c}(PQ) = \mathrm{c}(P)\,\mathrm{c}(Q) \pmod{A^\times}.$$

Démonstration. Si P et Q ne sont pas primitifs, disons $\mathrm{c}(P) = d$ et $\mathrm{c}(Q) = e$, alors on pose $\tilde{P} = P/d$ et $\tilde{Q} = Q/e$ qui sont primitifs. Il est clair que $\tilde{P}$ et $\tilde{Q}$ sont primitifs, que $PQ = de\tilde{P}\tilde{Q}$ et que $\mathrm{c}(\lambda P) = \mathrm{c}(R)$ pour R un polynôme et $\lambda \neq 0$. Il suffit donc de démontrer que $\mathrm{c}(\tilde{P}\tilde{Q}) = 1$.

Notons $\tilde{P} = a_0 + a_1X + \cdots + a_mX^m$ et $\tilde{Q} = b_0 + b_1X + \cdots + b_nX^n$. Supposons que $c(\tilde{P}\tilde{Q}) \neq 1$. Comme A est factoriel, $c(\tilde{P}\tilde{Q})$ admet un diviseur irréductible, disons $p \in A$. Cet élément irréductible ne peut pas diviser tous les coefficients de $\tilde{P}$, ni tous les coefficients de $\tilde{Q}$, donc il existe des rangs $i_0, j_0 \geq 0$ tels que :

$$p|a_0, \ldots, p|a_{i_0-1} \text{ mais } p \text{ ne divise pas } a_{i_0};$$
$$p|b_0, \ldots, p|b_{j_0-1} \text{ mais } p \text{ ne divise pas } b_{j_0}.$$

Or p divise les coefficients de $\tilde{P}\tilde{Q}$, donc en particulier le coefficient de $X^{i_0+j_0}$ qui vaut :

$$\sum_{i+j=i_0+j_0} a_ib_j = a_{i_0}b_{i_0} + \sum_{\substack{i+j=i_0+j_0 \\ i<i_0 \text{ ou } j<j_0}} \overbrace{a_ib_i}^{\text{divisible par } p}.$$

Comme la deuxième somme est divisible par p, on en déduit que p divise $a_{i_0}b_{j_0}$. Mais comme p est irréductible, il doit diviser a_{i_0} ou b_{j_0}, une contradiction. ◇

Ce lemme permet de déterminer les éléments irréductibles de $A[X]$. Leur description fait intervenir le corps des fractions K_A de A, défini dans la Section II.C.

Corollaire II.D.13. Soit A un anneau factoriel. Les éléments irréductibles de $A[X]$ sont :

- Les constantes $p \in A$ (polynômes de degré 0) qui sont irréductibles dans A ;
- Les polynômes $P \in A[X]$ de degré ≥ 1 primitifs et irréductibles dans $K_A[X]$.

Remarque II.D.14. Ce corollaire est faux si A n'est pas factoriel. Prenons par exemple $A = \mathbb{Q}[u, v]/(u^2 - v^3)$, qui n'est pas factoriel. Le polynôme $X^2 - v \in A[X]$ est unitaire. Il irréductible, car il n'a pas de racines (u n'est pas un carré dans A). Cependant, dans le corps des fractions de A, on a :

$$\left(\frac{u}{v}\right)^2 = \frac{u^2}{v^2} = \frac{v^3}{v^2} = v.$$

On trouve donc que $X^2 - v = (X - u/v)(X + u/v)$ est réductible sur le corps des fractions de A (qui est isomorphe à $\mathbb{Q}(t)$ via le morphisme $u \mapsto t^3$, $v \mapsto t^2$).

Démonstration. Commençons par démontrer que ces éléments sont bien irréductibles. Soit p est une constante irréductible dans A. Si on a une décomposition $p = QR$ dans $A[X]$, alors $\deg(Q) = \deg(R) = 0$ sont aussi des constantes, donc c'est une décomposition dans A et on doit avoir $Q \in A^\times = A[X]^\times$ ou $R \in A^\times = A[X]^\times$.

Supposons maintenant $P \in A[X]$ de degré non nul, primitif et irréductible dans $K_A[X]$ et supposons que $P = QR$ dans $A[X]$. Cette décomposition vaut aussi dans $K_A[X]$, donc l'un ou l'autre des facteurs appartient à $K_A[X]^\times = K_A \setminus \{0\}$. Quitte à échanger, on peut supposer que $Q = a \in K_A \setminus \{0\}$. Or $Q \in A[X]$ donc on a $a \in A$ et donc a divise $c(P) = 1$. C'est donc un élément inversible de A, donc de $A[X]$, et P est bien irréductible.

Démontrons maintenant que ce sont les seuls irréductibles. Soit $P \in A[X]$ irréductible. Si $\deg(P) = 0$, alors il est clair que $P \in A$ doit être irréductible dans A. Supposons maintenant que $\deg(P) \geq 1$. Comme $c(P)$ divise P, on doit avoir $c(P) = 1$ (sinon, P ne serait pas irréductible car divisible par $c(P)$). Démontrons enfin que P est irréductible dans $K_A[X]$.

Pour ce faire, supposons que $P = QR$ avec $Q, R \in K_A[X]$. En factorisant par les dénominateurs et par le PGCD des coefficients qui restent, on peut écrire $Q = \frac{a}{b}\tilde{Q}$ avec $a, b \in A$ premiers entre eux, $\tilde{Q} \in A[X]$ et $\mathrm{c}(\tilde{Q}) = 1$. De la même manière, factorisons $R = \frac{c}{d}\tilde{R}$. On a alors :

$$P = QR = \frac{ac}{bd}\tilde{Q}\tilde{R} \Longrightarrow bdP = ac\tilde{Q}\tilde{R}.$$

D'après le lemme de Gauss, on a

$$bd = \mathrm{c}(bd \cdot P) = \mathrm{c}\big(ac \cdot \tilde{Q}\tilde{R}\big) = ac \cdot \mathrm{c}\big(\tilde{Q}\tilde{R}\big) = ac \pmod{A^\times}.$$

On en déduit que $P = \frac{ac}{bd}\tilde{Q}\tilde{R} = u\tilde{Q}\tilde{R}$ où $u \in A^\times$ est inversible. Or, on a supposé que P est irréductible dans $A[X]$, donc l'un des facteurs $\tilde{Q}$ et $\tilde{R}$ est dans $A[X]^\times = A^\times \subset K_A[X]^\times$. Le polynôme P est donc bien irréductible dans $K_A[X]$. ◇

Démonstration du théorème de Gauss. Nous pouvons maintenant terminer de démontrer que $A[X]$ est factoriel. Commençons par montrer que tout polynôme non nul P est associé à un produit d'irréductibles. Si $d = \mathrm{c}(P)$, on a $P = dP'$ où P' est primitif. L'anneau $K_A[X]$ est principal, donc factoriel, et on peut décomposer P' en un produit d'irréductibles dans $K_A[X]$:

$$P' = Q_1 \dots Q_r, \qquad Q_i \in K_A[X] \text{ irréductible.}$$

Comme ci-dessus, on peut factoriser $Q_i = \frac{a_i}{b_i}\tilde{Q}_i$ avec $a_i, b_i \in A$ premiers entre eux et $\tilde{Q}_i \in A[X]$ primitif. Le polynôme $\tilde{Q}_i$ est associé à Q_i qui est irréductible dans $K_A[X]$; il est donc lui-même irréductible dans $K_A[X]$ et par suite dans $A[X]$ grâce au résultat précédent. On a de plus :

$$P = dP' = \frac{da_1 \dots a_r}{b_1 \dots b_r}\tilde{Q}_1 \dots \tilde{Q}_r.$$

En passant aux contenus, on voit que $u = \frac{da_1 \dots a_r}{b_1 \dots b_r}$ est un élément inversible de A, donc P est bien associé au produit d'irréductibles $\tilde{Q}_1 \dots \tilde{Q}_r$.

Grâce au critère de la **Proposition II.B.43**, pour conclure, il suffit de montrer que si $P \in A[X]$ est un polynôme irréductible, alors l'idéal (P) est premier. Il y a deux cas à considérer. Soit $\deg(P) = 0$, c.-à-d., $P = a \in A$ est une constante irréductible. Comme A est factoriel, $\mathfrak{p} = (a) \subset A$ est premier et donc $A[X]/(P) = (A/\mathfrak{p})[X]$ est intègre.

Sinon, $\deg(P) \geq 1$, $c(P) = 1$ et P est irréductible dans $K_A[X]$. On a un diagramme d'anneaux :

$$\begin{array}{ccc} A[X] & \hookrightarrow & K_A[X] \\ \downarrow & & \downarrow \\ A[X]/(P) & \overset{\iota}{\hookrightarrow} & K_A[X]/(P). \end{array}$$

Il suffit de prouver que ι est injective, car $K_A[X]/(P)$ est intègre (P est irréductible et $K_A[X]$ est principal dans (P) est premier) et un sous-anneau d'un anneau intègre est intègre. Cela revient à montrer que $(P \cdot K_A[X]) \cap A[X] = P \cdot A[X]$.

Il est clair que $P \cdot A[X] \subset (P \cdot K_A[X]) \cap A[X]$. Si maintenant on a $Q = PR$ avec $R \in K_A[X]$ et $Q \in A[X]$. Comme précédemment, on peut écrire $R = \frac{a}{b}R'$ avec $a, b \in A$ premiers entre eux, $R' \in A[X]$ primitif. On peut aussi factoriser $Q = c\tilde{Q}$ avec $\tilde{Q} \in A[X]$ primitif. On en déduit que $cb\tilde{Q} = aP\tilde{R}$, ce qui entraîne (en passant aux contenus) que b divise a ; or, ils sont premiers entre eux, donc b est inversible et $R \in$

$A[X]$. On a donc bien $Q \in P \cdot A[X]$. Le morphisme ι est donc injectif, donc $A[X]/(P)$ est intègre et (P) est premier.

Grâce au critère, on en déduit finalement que $A[X]$ est factoriel. ◇

Corollaire II.D.15. Si A est un anneau factoriel, alors $A[X_1, \dots, X_n]$ l'est aussi.

Démonstration. Appliquer le théorème de Gauss par récurrence. ◇

Corollaire II.D.16. Si A est factoriel, alors l'anneau $A[X_1, \dots, X_n, \dots]$ des polynômes en une infinité de variables est également factoriel.

Démonstration. Une décomposition en facteurs premiers ne fait intervenir qu'un nombre fini de variables. ◇

Exemple II.D.17. Les anneaux $\mathbb{Z}[X]$ et $\mathbb{R}[X, Y]$ sont factoriels sans être principaux.

Section II.E. Irréductibilité dans $\mathbb{Z}[x]$ et $\mathbb{Q}[x]$

Dans cette section, nous allons donner des critères pour déterminer si un polynôme est irréductible dans l'anneau factoriel $\mathbb{Z}[X]$.

Outre l'importance théorique de l'irréductibilité des polynômes, cette notion est également utile en cryptographie ! La clé de voûte de l'algorithme de chiffrement AES, par exemple, est l'utilisation du polynôme $P_{\text{AES}} = X^8 + X^4 + X^3 + X + 1$. Ce polynôme est irréductible dans $\mathbb{F}_{2^8}[X]$, où $\mathbb{F}_{2^8}$ est le corps à $2^8 = 256$ éléments (qui sera étudié dans le Chapitre IV). Pour cet algorithme, un bloc consiste en une matrice de 4×4 octets, dont les colonnes sont vues comme les coefficients d'un polynôme $b_0 + b_1X + b_2X^2 + b_3X^3$. L'une des étapes de l'algorithme est la multiplication de chaque colonne par un polynôme fixé, modulo P_{AES}. L'irréductibilité de P_{AES} nous assure que l'anneau quotient $\mathbb{F}_{2^8}[X]/(P_{\text{AES}})$ est intègre, donc la multiplication par un polynôme non nul mod P_{AES} est injective.

Nous avons vu dans le **Corollaire II.D.13** un critère pratique pour s'assurer de l'irréductibilité d'un polynôme. Rappelons-le ici, spécialisé au cas $A = \mathbb{Z}$ (dont le corps des fractions est $K_{\mathbb{Z}} = \mathbb{Q}$).

Proposition II.E.1. Les éléments irréductibles de $\mathbb{Z}[X]$ sont :

- Les constantes $p \in \mathbb{Z} \subset \mathbb{Z}[X]$ qui sont des nombres premiers au signe près ;
- Les polynômes $P \in \mathbb{Z}[X]$ de degré ≥ 1 qui sont primitifs et irréductibles dans $\mathbb{Q}[X]$.

Déterminer les polynômes irréductibles non-constants de $\mathbb{Z}[X]$ revient donc à déterminer les polynômes irréductibles de $\mathbb{Q}[X]$ (quitte à factoriser les coefficients d'un polynôme par leur PGCD). Commençons par quelques propriétés faciles des polynômes irréductibles.

Exemple II.E.2. Soit $a \in \mathbb{K}$ un élément d'un corps $\mathbb{K}$. Le polynôme $X - a$ est irréductible dans $\mathbb{K}[X]$. En prenant $\mathbb{K} = \mathbb{Q} = K_{\mathbb{Z}}$, on trouve que si $a \in \mathbb{Z}$, alors $X - a$ irréductible dans $\mathbb{Z}[X]$.

Proposition II.E.3. Soit $\mathbb{K}$ un corps. Un polynôme irréductible $P \in \mathbb{K}[X]$ de degré ≥ 2 n'a pas de racine dans $\mathbb{K}$.

Démonstration. Supposons au contraire que $P \in \mathbb{K}[X]$ a une racine $a \in \mathbb{K}$. L'anneau $\mathbb{K}[X]$ est euclidien, donc on peut effectuer la division euclidienne de P par $X - a$ et écrire $P = (X - a)Q + r$ où $r \in \mathbb{K}$. Mais alors, si on évalue en $X = a$, on trouve $P(a) = (a - a)\,Q(a) + r$ donc $r = 0$ et $X - a$ (qui est irréductible) divise P, qui n'est donc pas irréductible (car $\deg(Q) \geq 1$ n'est pas inversible non plus). ◇

Remarque II.E.4. Un polynôme réductible dans $\mathbb{K}[X]$ n'a pas nécessairement de racine : par exemple, $X^4 + 2X^2 + 1 = (X^2 + 1)^2$ est réductible mais n'a pas de racine dans $\mathbb{R}$.

Remarque II.E.5. Un polynôme réductible $P \in \mathbb{K}[X]$ de degré ≤ 3 admet nécessairement une racine (l'un des deux facteurs dans la décomposition est de degré 1).

Remarque II.E.6. Un polynôme irréductible dans $\mathbb{Q}[X]$ peut avoir une racine réelle : par exemple, $X^2 - 2$ est irréductible dans $\mathbb{Q}[X]$ mais admet $\sqrt{2}$ pour racine.

La recherche de racines rationnelles est simplifiée par le résultat suivant, qui permet de réduire le nombre de rationnels à considérer à un nombre fini (quoique souvent très grand) :

Proposition II.E.7. Soit $P = a_0 + a_1X^1 + \cdots + a_nX^n \in \mathbb{Q}[X]$ un polynôme à coefficients rationnels. Si $\alpha = p/q \in \mathbb{Q}$ est une racine rationnelle de P avec $p \wedge q = 1$, alors p divise a_0 et q divise a_n.

En effet, si $P(p/q) = 0$, alors :

$$a_0 + \frac{a_1 p}{q} + \frac{a_2 p^2}{q^2} + \cdots + \frac{a_n p^n}{q^n} = 0$$
$$\Longrightarrow q^n a_0 + a_1 p q^{n-1} + a_2 p^2 q^{n-2} + \cdots a_n p^n = 0.$$

Comme q divise tous les termes sauf le dernier, il divise aussi $a_n p^n$; comme q et p sont premiers entre eux, q divise donc a_n. De la même manière, p divise a_0. ◇

Exemple II.E.8. Soit $P = 2X^3 + X^2 + 3$. Les racines rationnelles de P sont à chercher dans l'ensemble suivant :

$$\{\pm 1/1, \pm 3/1, \pm 1/2, \pm 3/2\}.$$

Aucun de ces nombres n'est une racine de P. Comme $\deg(P) = 3$, il est donc irréductible sur $\mathbb{Q}$ (car sinon il aurait une racine).

En Mathematica :

```
irréductible[q_, x_] := Module[{a0, a3, candidats},
  a0 = Coefficient[q, x, 0];
  a3 = Coefficient[q, x, 3];
  candidats =
    Table[εu/v, {ε, {-1, 1}}, {u, Divisors[a0]}, {v,
Divisors[a3]}];
  FreeQ[(q /. {x -> #1} &) /@ candidats, 0]
]
```

La proposition précédente donne un algorithme pour vérifier si un polynôme à coefficients rationnels a une racine, et donc vérifier s'il est irréductible si son degré est ≤ 3. Il y a cependant plusieurs problèmes :

- L'algorithme ne marche que pour les polynômes de bas degré (si ce qui nous intéresse est l'irréductibilité) ;
- Il nécessite de vérifier un grand nombre de candidats, à savoir $2 \times |\{\text{diviseurs de } a_0\}| \times |\{\text{diviseurs de } a_n\}|$. Le nombre de diviseurs $\mathrm{d}(n)$ vaut $\ln(n)$ « en moyenne[9] » ;

[9] Un théorème de Dirichlet dit que (où $\gamma = \lim_{n\to\infty}\left(\left(\sum_{k=1}^{n} 1/k\right) - ln(n)\right) \approx 0{,}577$ est la constante d'Euler) :

$$\sum_{n\leq x} d(x) = x\ln(x) + (2\gamma - 1)x + O\left(\sqrt{x}\right).$$

- Calculer $P(x)$ demande un grand nombre d'opérations en général ;
- Une racine de P est un « témoin » pour la réductibilité, mais il n'y a pas de « témoin » pour l'irréductibilité : même quand on sait qu'un polynôme est irréductible, on ne peut pas faire mieux que recalculer $P(x)$ pour tous les candidats racines pour le revérifier.

Notre objectif est maintenant de faire mieux. Rappelons le résultat suivant, bien connu :

Théorème II.E.9 (« Théorème fondamental de l'algèbre », Théorème de D'Alembert–Gauss). Tout polynôme non constant de $\mathbb{C}[X]$ admet une racine. Par conséquent, les seuls polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1 (associés à un polynôme de la forme $X - a$ avec $a \in \mathbb{C}$).

Corollaire II.E.10. Les seuls polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1, et les polynômes de degré 2 qui n'ont pas de racines (c.-à-d. dont le discriminant est strictement négatif).

L'irréductibilité dans $\mathbb{Q}[X]$ est bien plus difficile à caractériser. Le théorème suivant donne un critère, qui s'applique à n'importe quel anneau factoriel (et en particulier à $A = \mathbb{Z}$) :

Théorème II.E.11 (Critère d'Eisenstein). Soit $P = a_0 + a_1X + \cdots + a_nX^n \in A[X]$ un polynôme à coefficients dans un anneau factoriel A, avec $a_n \neq 0$. Soit $p \in A$ un élément irréductible. Supposons que toutes les propriétés suivantes soient vérifiées :

(a) L'élément p ne divise pas a_n ;
(b) Pour tout $i < n$, l'élément p divise a_i ;
(c) L'élément p^2 ne divise pas a_0.

Alors P est irréductible dans $K_A[X]$, et donc dans $A[X]$ si $c(P) = 1$.

Remarque II.E.12. Dans l'esprit des tests de primalité, on peut appeler p un « témoin » d'irréductibilité.

En termes algorithmiques, ce critère donne :

```
eisenstein[p_, x_] := Module[{coeffs, dom, const, candidats},
  coeffs = CoefficientList[p, x];
  dom = Last[coeffs];
  const = First[coeffs];
  candidats = FactorInteger[#][[All, 1]] & /@ Most[coeffs];
  Length[candidats] >= 1 && (
    candidats = Intersection @@ candidats;
    candidats = Select[candidats, ! Divisible[const, #^2] &];
    candidats = Select[candidats, ! Divisible[dom, #] &];
    Length[candidats] >= 1
    )
  ]
```

Exercice II.E.13. Démontrer que $4X^3 + 21X^2 + 81X + 15$ est irréductible dans $\mathbb{Z}[X]$.

Exercice II.E.14. Démontrer que $X^4 + 1$ est irréductible sur $\mathbb{Z}$ mais est réductible mod p pour tout p.

Exercice II.E.15. Soit p un nombre premier. Démontrer que $1 + X + \cdots + X^{p-1}$ est irréductible. (Indice : poser $X = Y + 1$).

La technique de l'exercice précédent est très utile pour appliquer le critère d'Eisenstein. Souvent, même si $P \in \mathbb{Z}[X]$ est irréductible, le critère ne s'applique pour aucun nombre premier p. Mais en décalant la variable $X = Y + a$ astucieusement (ce qui ne change pas la réductibilité), il est possible de faire en sorte que le critère s'applique.

Exercice II.E.16. Soit $a = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ un entier et sa décomposition en facteurs premiers. Si l'un des α_i vaut 1, alors $X^n - a$ est irréductible pour $n \geq 1$.

Remarque II.E.17. Bien que ce théorème soit généralement utilisé pour $A = \mathbb{Z}$, on peut bien sûr l'utiliser pour d'autres anneaux factoriels. On peut par exemple l'appliquer à $A = \mathbb{K}[X]$ (dont le corps de fractions est $\mathbb{K}(X)$) pour étudier l'irréductibilité de polynômes à deux variables, c'est-à-dire les éléments de $\mathbb{K}[X,Y] = (\mathbb{K}[X])[Y]$.

Par exemple, si $\lambda \notin \{0,1\}$, alors $P = Y^2 - X(X-1)(X-\lambda)$ est irréductible dans $\mathbb{K}[X,Y]$ (en choisissant l'élément irréductible $X \in \mathbb{K}[X]$ pour appliquer le critère, par exemple). Dans ce cas, l'ensemble de ses racines s'appelle une « courbe elliptique ». Les courbes elliptiques sont à la base de d'algorithmes cryptographiques (ECDH, ECDSA…), dont les clés sont plus petites pour un niveau de sécurité équivalent que des algorithmes plus anciens tels que RSA.

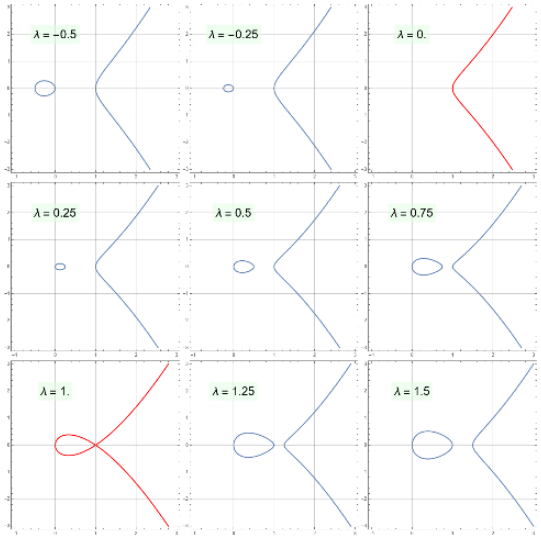


Figure II.E-a Les solutions de l'équation $y^2 = x(x-1)(x-\lambda)$ dans $\mathbb{R}^2$ pour quelques valeurs de λ. En rouge, les cas singuliers.

Démonstration du théorème. Supposons que $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ est un polynôme qui vérifie le critère du théorème pour un irréductible $p \in A$, mais que P est réductible dans $K_A[X]$. On peut donc écrire $P = QR$, avec $Q = \sum_{j=0}^{q} b_j X^j$, $R = \sum_{k=0}^{r} c_k X^k$, $q + r = n$ et $q, r > 0$.

L'anneau A est factoriel et p est irréductible, donc $\mathfrak{p} = (p) \subset A$ est premier d'après la **Proposition II.B.43**. L'anneau $B = A/\mathfrak{p}$ est donc intègre. (Attention, il n'est en général pas factoriel !)

Étant donné $a \in A$, notons $\bar{a} \in B$ son image mod $\mathfrak{p}$. Comme p divise tous les coefficients de P sauf le coefficient dominant, l'égalité $P = QR$ devient, mod $\mathfrak{p}$:

$$\bar{a}_n X^n = \left(\bar{b}_0 + \dots + \bar{b}_q X^q\right)(\bar{c}_0 + \dots + \bar{c}_r X^r). \qquad (*)$$

Comme $\bar{a}_n \neq 0$, on a également $\bar{b}_q, \bar{c}_r \neq 0$. Cette égalité reste vraie dans $K_B[X]$. Or, l'anneau $K_B[X]$ est principal (donc factoriel[10]), et X est irréductible. Par unicité de la décomposition en produits d'irréductibles, l'équation $(*)$ entraîne que X divise chacun des deux facteurs (ils ne sont pas inversibles car $q, r > 0$). En particulier, $\bar{b}_0 = \bar{c}_0 = 0$, c'est-à-dire p divise b_0 et c_0. Or on a $a_0 = b_0 c_0$, qui est donc divisible par p^2, ce qui contredit l'hypothèse du critère. ◇

[10] Comme B n'est en général pas factoriel, $B[X]$ non plus et nous devons passer par le corps des fractions de B.

Terminons par un dernier critère. Son importance sera plus claire une fois que nous en saurons plus sur les corps.

Théorème II.E.18. Soit A un anneau factoriel, $\mathfrak{p} \subset A$ un idéal premier, et $B = A/\mathfrak{p}$ le quotient (intègre), avec $a \mapsto \bar{a}$ l'application quotient. Soit $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ et $\bar{P}$ son image dans $B[X]$. Supposons que $\bar{a}_n \neq 0$ (donc $\deg(P) = \deg(\bar{P}) = n$). Si $\bar{P}$ est irréductible dans $B[X]$ ou dans $K_B[X]$, alors il est irréductible dans $K_A[X]$.

On peut résumer ce théorème par : « si la réduction mod $\mathfrak{p}$ d'un polynôme est irréductible, alors ce polynôme est irréductible (sur le corps des fractions) ».

Démonstration. Supposons que P vérifie les hypothèses et que $P = QR$ dans $A[X]$, où $Q = \sum_{j=0}^{q} b_j X^j$ et $R = \sum_{k=0}^{r} c_k X^k$. Comme $\bar{P} = \bar{Q}\bar{R}$, on a $\bar{a}_n = \bar{b}_q \bar{c}_r$ donc $\bar{b}_q, \bar{c}_r \neq 0$ et $\deg(Q) = \deg(\bar{Q})$ et $\deg(R) = \deg(\bar{R})$. Comme P est irréductible dans $B[X]$ (ou $K_B[X]$), l'un des polynômes $\bar{Q}$ ou $\bar{R}$ est de degré 0. Donc il en est de même pour l'un des polynômes Q ou R, qui est donc inversible dans $K_A[X]$. Le polynôme P est donc irréductible dans $K_A[X]$. ◇

Remarque II.E.19. Le polynôme P n'est pas nécessairement irréductible dans $A[X]$ (par exemple $P = 2X \in \mathbb{Z}[X]$ et $\mathfrak{p} = (3)$).

Remarque II.E.20. L'anneau $B = A/\mathfrak{p}$ n'est pas nécessairement factoriel. Un polynôme de degré non nul irréductible dans $B[X]$ n'est donc pas nécessairement irréductible dans $K_B[X]$, et on ne peut même pas définir la notion de polynôme primitif pour la réciproque.

Exercice II.E.21. Démontrer que le polynôme $X^2 + Y^2 + 1$ est irréductible dans $\mathbb{R}[X, Y]$. (Indice : prendre $A = \mathbb{R}[X]$ et $\mathfrak{p} = (X)$).

Exercice II.E.22. Démontrer que le polynôme $X^3 + 117X^2 - 136X + 91$ est irréductible sur $\mathbb{Z}$. Indice : poser $\mathfrak{p} = (3)$. On notera qu'on ne peut pas lui appliquer le critère d'Eisenstein.

Chapitre III. THÉORIE DES CORPS

« L'algèbre n'est qu'une géométrie écrite, la géométrie n'est qu'une algèbre figurée. »

Sophie Germain, *Pensées diverses*

Section III.A. Caractéristique et degré

§ III.A(a) Caractéristique d'un anneau

Définition III.A.1. Soit A un anneau et soit $\varphi\colon \mathbb{Z} \to A$ l'unique morphismes d'anneaux ($\varphi(n) = n \cdot 1$). L'idéal $\ker(\varphi) \subset \mathbb{Z}$ est principal et engendré par un unique élément positif $n \in \mathbb{N}$, appelé la *caractéristique* de l'anneau, noté $\operatorname{car}(A)$.

Cette définition recouvre plusieurs cas :

- Si $n = 0$, on a $\ker(\varphi) = (0) = 0$, c'est-à-dire $\varphi\colon \mathbb{Z} \to A$ est injectif. On dira alors que A est « de caractéristique nulle ».
- Si $n = 1$, alors $\ker(\varphi) = (1) = \mathbb{Z}$. Or $\varphi(1) = 1$, donc $0 = 1$ dans A, et donc A est l'anneau nul.
- Si $n \geq 2$, alors n est le plus petit entier positif tel que
$$n \cdot 1 = 1 + 1 + \cdots + 1 = 0.$$

Exemple III.A.2. L'anneau $\mathbb{Z}$ est de caractéristique nulle. Étant donné $n \geq 1$, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est de caractéristique n.

Proposition III.A.3. Si A est un anneau de caractéristique n, alors tout sous-anneau de A est de caractéristique n.

Démonstration. Supposons que $\iota\colon B \hookrightarrow A$ est un sous-anneau. Alors $\varphi\colon \mathbb{Z} \to A$ se factorise par l'unique morphisme $\varphi\colon \mathbb{Z} \to B$ avec $\varphi \circ \iota = \varphi$. Comme ι est injective, il n'est pas difficile de voir que $\ker(\varphi) = \ker(\varphi')$, donc les deux noyaux sont engendrés par le même élément positif. ◇

Proposition III.A.4. Soit A un anneau intègre. Sa caractéristique est soit nulle, soit un nombre premier.

Démonstration. Supposons que $\operatorname{car}(A) = n \neq 0$ se décompose en un produit $n = ab$. Comme $\varphi\colon \mathbb{Z} \to A$ est un morphisme d'anneaux, on a :
$$n \cdot 1 = \varphi(n) = \varphi(ab) = \varphi(a)\varphi(b) = (a \cdot 1)(b \cdot 1).$$
L'un des deux facteurs est donc nul, car A est intègre ; quitte à échanger, disons $a \cdot 1 = 0$, ou en d'autres termes, $a \in \ker(\varphi)$. Or par définition de la caractéristique, $\ker(\varphi) = (n)$, donc n divise son diviseur a, et par suite $a = \pm n$ et $b = \pm 1$. ◇

Cette proposition est souvent appliquée aux corps, qui sont des anneaux intègres. Leur caractéristique est donc soit nulle, soit un nombre premier.

§ III.A(b) Extensions de corps

On rappelle que tout morphisme entre deux corps est automatiquement injectif. Cela justifie la définition suivante :

Définition III.A.5. Soit $\mathbb{K}$ un corps. Une *extension (de corps)* de $\mathbb{K}$ est un corps $\mathbb{L}$ muni d'un morphisme (injectif) $\mathbb{K} \to \mathbb{L}$. Si $\mathbb{L}$ est une extension de $\mathbb{K}$, alors on peut voir $\mathbb{K}$ comme un sous-corps de $\mathbb{L}$ et on notera souvent $\mathbb{K} \subset \mathbb{L}$ pour une extension de corps.

Exemple III.A.6. On a les extensions de corps suivantes : $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, $\mathbb{Q} \subset \mathbb{Q}[i]$, $\mathbb{K} \subset \mathbb{K}(X)$, etc.

Remarque III.A.7. Il peut exister plusieurs manières de plonger un corps dans un autre. Par exemple, on peut inclure $\mathbb{K}(X)$ dans $\mathbb{K}(Y,Z)$ d'au moins deux façons différentes (en envoyant X sur Y ou sur Z). Même si la notation pourrait faire croire le contraire, la donnée du morphisme concret $\mathbb{K} \to \mathbb{L}$ fait partie intégrante de la notion d'extension. Elle est simplement tacite dans la notation.

La proposition suivante est immédiate et ne constitue qu'un petit exercice de réécriture des définitions :

Proposition III.A.8. Si $\mathbb{K} \subset \mathbb{L}$ est une extension de corps, alors $\mathbb{L}$ est muni d'une structure de $\mathbb{K}$-espace vectoriel telle que l'inclusion $\mathbb{K} \subset \mathbb{L}$ soit $\mathbb{K}$-linéaire.

On peut également relier la notion d'extension et la notion de caractéristique (notée $\mathrm{car}(\mathbb{K})$).

Définition III.A.9. On appelle *sous-corps premier* d'un corps $\mathbb{K}$ le plus petit sous-corps de $\mathbb{K}$.

Proposition III.A.10. Soit $\mathbb{K}$ un corps.

- Si $\mathrm{car}(\mathbb{K}) = 0$, alors son sous-corps premier est $\mathbb{Q}$.
- Si $\mathrm{car}(\mathbb{K}) = p > 0$ (forcément un nombre premier), alors son sous-corps premier est $\mathbb{Z}/p\mathbb{Z}$.

Démonstration. Si $\mathrm{car}(\mathbb{K}) = 0$, l'unique morphisme $\mathbb{Z} \to \mathbb{K}$ est injectif et s'étend donc en un morphisme $K_{\mathbb{Z}} = \mathbb{Q} \to \mathbb{K}$. Si au contraire $\mathrm{car}(\mathbb{K}) = p > 0$, ce morphisme a pour noyau (p) et factorise par un morphisme d'anneaux $\mathbb{Z}/p\mathbb{Z} \to \mathbb{K}$, et $\mathbb{Z}/p\mathbb{Z}$ est un corps donc il s'agit d'une extension. ◇

Enfin, on a la notion suivante qui permet de relier les extensions entre elles.

Définition III.A.11. Soit $\mathbb{K}$ un corps et $\mathbb{K} \subset \mathbb{L}$, $\mathbb{K} \subset \mathbb{L}'$ des extensions de $\mathbb{K}$. Un *$\mathbb{K}$-morphisme* de $\mathbb{L}$ dans $\mathbb{L}'$ est un morphisme de corps $f : \mathbb{L} \to \mathbb{L}'$ tel que $\forall x \in \mathbb{K}, f(x) = x$.

Remarque III.A.12. La condition d'être un $\mathbb{K}$-morphisme est équivalent à la condition d'être un morphisme de $\mathbb{K}$-algèbres. La terminologie est simplement différente pour les extensions de corps.

Exemple III.A.13. La conjugaison complexe $z \mapsto \bar{z}$ définit un $\mathbb{R}$-morphisme $\mathbb{C} \to \mathbb{C}$.

§ III.A(c) Degré d'une extension

Définition III.A.14. Soit $\mathbb{K} \subset \mathbb{L}$ une extension de corps. Si la dimension de $\mathbb{L}$ vu comme $\mathbb{K}$-espace vectoriel $\dim_{\mathbb{K}} \mathbb{L}$ est finie, alors on dit que l'extension est *finie*, on appelle cette dimension le *degré* de l'extension et on la note $[\mathbb{L} : \mathbb{K}]$. Si la dimension est infinie, on pose $[\mathbb{L} : \mathbb{K}] = \infty$.

Exemple III.A.15. Il est bien connu que $[\mathbb{C} : \mathbb{R}] = 2$. En revanche, $[\mathbb{R} : \mathbb{Q}] = \infty$ (car un $\mathbb{Q}$-espace vectoriel de dimension finie est dénombrable, mais $\mathbb{R}$ ne l'est pas).

Corollaire III.A.16. Si $\mathbb{K} \subset \mathbb{L}$ est une extension de corps et $\mathbb{K}$ et $\mathbb{L}$ sont tous les deux finis, alors on a $|\mathbb{L}| = |\mathbb{K}|^n$ où $n = [\mathbb{L} : \mathbb{K}]$.

Corollaire III.A.17. Si $\mathbb{K}$ est un corps fini, alors son cardinal est une puissance d'un nombre premier.

Démonstration. Si $\mathbb{K}$ est fini, alors sa caractéristique p est non-nulle (car sinon le corps contiendrait $\mathbb{Z}$ qui est de cardinal infini). Donc $\mathbb{K}$ est une extension de $\mathbb{Z}/p\mathbb{Z}$ et son cardinal est donc une puissance de $|\mathbb{Z}/p\mathbb{Z}| = p$. ◇

Exemple III.A.18. Ce corollaire permet de démontrer qu'il n'existe pas de corps de cardinal 6.

Théorème III.A.19. Soit $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ des extensions de corps. On a l'équation suivante :

$$[\mathbb{M}:\mathbb{K}] = [\mathbb{M}:\mathbb{L}] \cdot [\mathbb{L}:\mathbb{K}].$$

En particulier, $\mathbb{K} \subset \mathbb{M}$ est finie si et seulement si $\mathbb{K} \subset \mathbb{L}$ et $\mathbb{L} \subset \mathbb{M}$ le sont.

Démonstration. Soit $(e_i)_{i\in I}$ une base de $\mathbb{L}$ sur $\mathbb{K}$ et $(f_j)_{j\in J}$ une base de $\mathbb{M}$ sur $\mathbb{L}$. Démontrons que la famille $(e_i f_j)_{i\in I, j\in J}$ est une base de $\mathbb{M}$ sur $\mathbb{K}$.

- Elle est libre : si $\sum_{i,j} \lambda_{i,j} e_i f_j = 0$ dans $\mathbb{M}$, alors la combinaison linéaire $\sum_j (\sum_i \lambda_{i,j} e_i) f_j$ à coefficients dans $\mathbb{L}$ est nulle. Or, (f_j) est libre donc pour tout j, $\sum_i \lambda_{i,j} e_i = 0$. Mais la famille $(e_i)_i$ est également libre, donc pour tout i, j, on a $\lambda_{i,j} = 0$.
- Elle est génératrice : si $x \in \mathbb{M}$, alors il existe des coefficients (μ_j) dans $\mathbb{L}$ tels que $x = \sum_j \mu_j f_j$, car (f_j) engendre $\mathbb{M}$ en tant que $\mathbb{L}$-espace vectoriel. De la même manière, pour chaque j, il existe des coefficients $(\lambda_{i,j})$ tels que $\mu_j = \sum_i \lambda_{i,j} e_i$. On en déduit que $x = \sum_{i,j} \lambda_{i,j} e_i f_j$.

On conclut en calculant le cardinal de la base ainsi obtenue. ◇

Comparer la définition suivante à la **Définition II.A.36**.

Définition III.A.20. Soit $\mathbb{K} \subset \mathbb{L}$ une extension de corps et $\alpha \in \mathbb{L}^*$ un élément. On note $\mathbb{K}(\alpha)$ le plus petit sous-corps de $\mathbb{L}$ qui contient $\mathbb{K}$ et α et on l'appelle le *sous-corps engendré par α*. Si $\alpha_1, \dots, \alpha_n \in \mathbb{L}$, on définit $\mathbb{K}(\alpha_1, \dots, \alpha_n)$ de façon similaire.

Définition III.A.21. Une extension de corps $\mathbb{K} \subset \mathbb{L}$ est *monogène* s'il existe $\alpha \in \mathbb{L} \setminus \mathbb{K}$ tel que $\mathbb{L} = \mathbb{K}(\alpha)$. Dans ce cas, on appelle α un *élément primitif*.

Remarque III.A.22. En général, $\mathbb{K}(\alpha) \neq \mathbb{K}[\alpha]$ et $\mathbb{K}(\alpha)$ n'est pas le corps des fractions de $\mathbb{K}[\alpha]$. La proposition suivante est claire (comparer avec la définition de $\mathbb{K}[\alpha]$) :

Proposition III.A.23. Soit $\mathbb{K} \subset \mathbb{L}$ une extension de corps et $\alpha \in \mathbb{L}$, on a :

$$\mathbb{K}(\alpha) = \left\{ y \in \mathbb{L} \;\middle|\; \exists P, Q \in \mathbb{K}[X],\ Q(\alpha) \neq 0 \text{ et } y = \frac{P(\alpha)}{Q(\alpha)} \right\}.$$

§ III.A(d) Éléments algébriques et transcendants

La distinction entre $\mathbb{K}[\alpha]$ et $\mathbb{K}(\alpha)$ motive la définition suivante :

Définition III.A.24. Soit $\mathbb{K} \subset \mathbb{L}$ une extension de corps et $\alpha \in \mathbb{L}$. Soit $\varphi_\alpha : \mathbb{K}[X] \to \mathbb{L}$ l'unique morphisme de $\mathbb{K}$-algèbres tel que $\varphi_\alpha(X) = \alpha$.

- On dit que α est *transcendant* (sur $\mathbb{K}$) si φ_α est injectif.
- Sinon, on dit que α est *algébrique* (sur $\mathbb{K}$).

Exemple III.A.25. L'élément $\sqrt{2} \in \mathbb{R}$ est algébrique sur $\mathbb{Q}$, car il est racine de $P = X^2 - 2$. De la même manière, $\exp(2i\pi/3)$ est algébrique sur $\mathbb{Q}$ car il est racine de $X^3 - 1$. Les nombres réels e et π sont transcendants sur $\mathbb{Q}$ (théorèmes d'Hermite et von Lindemann, respectivement, voir la Section III.C).

Exercice III.A.26. Soit $\mathbb{K}$ un corps. L'élément $X \in \mathbb{K}(X)$ est transcendant sur $\mathbb{K}$.

Exemple III.A.27. Si $\mathbb{K} \subset \mathbb{L}$ et $\alpha \in \mathbb{K} \subset \mathbb{L}$, alors α est algébrique sur $\mathbb{K}$ (car racine de $X - \alpha$).

Remarque III.A.28. Si $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ sont des extensions, et si $\alpha \in \mathbb{M}$ est algébrique sur $\mathbb{K}$, alors il est algébrique sur $\mathbb{L}$ (et par contraposée, s'il est transcendant sur $\mathbb{L}$ alors il l'est aussi sur $\mathbb{K}$). Cependant, il est possible que α soit algébrique sur $\mathbb{L}$ mais pas sur $\mathbb{K}$.

Exemple III.A.29. Considérons $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. Le nombre $e + i\pi$ est algébrique sur $\mathbb{R}$ (il est racine de $(X - e)^2 + \pi^2 = 0$) mais il est transcendant sur $\mathbb{Q}$.

Si un nombre est algébrique sur un sous-corps, alors c'est la racine de nombreux polynômes : par exemple, $\sqrt{2} \in \mathbb{R}$ est racine de $X^2 - 2$, mais aussi de $X^4 - 4$, etc. Parmi ces polynômes, l'un d'entre eux est distingué :

Définition III.A.30. Soit $\mathbb{K} \subset \mathbb{L}$ une extension, α un élément algébrique sur $\mathbb{K}$, et $\varphi_\alpha \colon \mathbb{K}[X] \to \mathbb{L}$ l'évaluation en α. Le noyau de φ_α est principal (car $\mathbb{K}[X]$ l'est). Si $\ker(\varphi_\alpha) = (P)$ avec $P \in \mathbb{K}[X]$ unitaire (de coefficient dominant égal à 1), on dit que P est le *polynôme minimal* de α et on le note $\mathrm{Irr}_{\mathbb{K}}(\alpha)$.

Exemple III.A.31. Le polynôme minimal de $\sqrt{2} \in \mathbb{R}$ sur $\mathbb{Q}$ est $\mathrm{Irr}_{\mathbb{Q}}(\sqrt{2}) = X^2 - 2$. Le polynôme minimal de $j \coloneqq \exp(2i\pi/3)$ sur $\mathbb{Q}$ est $\mathrm{Irr}_{\mathbb{Q}}(j) = 1 + X + X^2$.

Remarque III.A.32. Le polynôme minimal dépend bien sûr du corps dans lequel on se place. Par exemple, $\mathrm{Irr}_{\mathbb{R}}(\sqrt{2}) = X - \sqrt{2}$. Cependant, on a le résultat suivant :

Proposition III.A.33. Soit $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ une suite d'extensions et $\alpha \in \mathbb{L}$ un élément quelconque. Alors le polynôme $\mathrm{Irr}_{\mathbb{L}}(\alpha)$ divise le polynôme $\mathrm{Irr}_{\mathbb{K}}(\alpha)$ dans $\mathbb{L}[X]$.

Démonstration. Le polynôme $\mathrm{Irr}_{\mathbb{K}}(\alpha)$, qui est à coefficients dans $\mathbb{K}$, peut également être vu comme un polynôme à coefficients dans $\mathbb{L}$. Comme il s'annule en α, il appartient au noyau de $\varphi_\alpha \colon \mathbb{L}[X] \to \mathbb{M}$. Or, par définition, ce noyau est engendré par $\mathrm{Irr}_{\mathbb{L}}(\alpha)$, qui divise donc $\mathrm{Irr}_{\mathbb{K}}(\alpha)$. ◇

Lemme III.A.34. Le polynôme minimal d'un élément algébrique est irréductible.

Démonstration. Supposons au contraire que le polynôme minimal $P = QR \in \mathbb{K}[X]$ d'un élément algébrique $\alpha \in \mathbb{L}$ soit réductible. Alors $P(\alpha) = 0$ donc $Q(\alpha)\,R(\alpha) = 0$ donc au moins l'un des facteurs est nul, disons $Q(\alpha) = 0$. On a donc $Q \in (P)$ avec Q qui divise strictement P, c'est absurde. ◇

La dichotomie entre éléments algébriques et transcendants est illustré par les résultats suivants :

Proposition III.A.35. Soit $\mathbb{K} \subset \mathbb{L}$ une extension et $\alpha \in \mathbb{L}$ un élément transcendant sur $\mathbb{K}$. Alors $\mathbb{K}[\alpha]$ est isomorphe à $\mathbb{K}[X]$ et $\mathbb{K}(\alpha)$ est isomorphe à $\mathbb{K}(X)$.

Démonstration. Cela découle directement du fait que $\varphi_\alpha \colon \mathbb{K}[X] \to \mathbb{L}$ est injectif d'image $\mathbb{K}[\alpha]$, et que $\mathbb{K}(\alpha)$ est l'image de $\mathbb{K}(X) \to \mathbb{L}$, $X \mapsto \alpha$ (qui est bien défini car α est transcendant). ◇

Proposition III.A.36. Soit $\mathbb{K} \subset \mathbb{L}$ une extension et $\alpha \in \mathbb{L}$. Les propositions suivantes sont équivalentes :

(a) L'élément α est algébrique sur $\mathbb{K}$.
(b) On a l'égalité $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$.
(c) La dimension de $\mathbb{K}[\alpha]$ comme $\mathbb{K}$-espace vectoriel, $\dim_{\mathbb{K}} \mathbb{K}[\alpha]$, est finie.

Démonstration. Démontrons que (a) ⇒ (b). On a $\mathbb{K}[\alpha] = \mathbb{K}[X]/(P)$ où P est le polynôme minimal de α. Le polynôme P est irréductible et $\mathbb{K}[\alpha]$ est principal, donc (P) est maximal et $\mathbb{K}[\alpha]$ est un corps. Comme $\mathbb{K}[\alpha] \subset \mathbb{K}(\alpha)$ et $\mathbb{K}(\alpha)$ est le plus petit corps contenant α, on a bien $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$. Réciproquement, si $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$ alors α est algébrique (car s'il était transcendant, ces deux anneaux seraient différents), donc (b) ⇒ (a). De la même manière, (c) ⇒ (a), car si α était transcendant, alors $\mathbb{K}[\alpha] \cong \mathbb{K}[X]$ serait de dimension infinie.

Enfin, démontrons que (a) ⇒ (c). L'espace vectoriel $\mathbb{K}[\alpha]$ est isomorphe à $\mathbb{K}[X]/(P)$. Si on note $P = \sum_{i=0}^{n-1} a_i X^i + X^n$, alors on peut montrer facilement par récurrence que $\{1, X, X^2, \dots, X^{n-1}\}$ est une base du quotient comme $\mathbb{K}$-espace vectoriel, donc $\dim_{\mathbb{K}} \mathbb{K}[\alpha] = \deg(P) < \infty$. ◇

Définition III.A.37. Soit $\mathbb{K} \subset \mathbb{L}$ et $\alpha \in \mathbb{L}$ un élément algébrique. La dimension $\dim_{\mathbb{K}} \mathbb{K}[\alpha]$, qui est égale au degré du polynôme minimal de α, s'appelle le *degré* de α (sur $\mathbb{K}$).

Remarque III.A.38. Le degré d'un élément dépend bien entendu de l'extension de corps. Par exemple, $\sqrt[4]{2}$ est de degré 4 sur $\mathbb{Q}$ (son polynôme minimal est $X^4 - 2$) mais il est de degré 2 sur $\mathbb{K}[\sqrt{2}]$ (son polynôme minimal est $X^2 - \sqrt{2}$).

Section III.B. Clôture et rupture

Commençons par quelques rappels élémentaires sur les racines des polynômes.

Définition III.B.1. Soit $\mathbb{K} \subset \mathbb{L}$ une extension de corps, $P \in \mathbb{K}[X]$ un polynôme, et $\alpha \in \mathbb{L}$ une racine de P. La *multiplicité* de α est le plus grand entier n tel que $(X - \alpha)^n$ divise P dans $\mathbb{L}[X]$. Si cette multiplicité vaut 1, on dit que α est une *racine simple*, sinon on dit que α est une *racine multiple*.

Remarque III.B.2. Comme $\mathbb{L}[X]$ est factoriel, on peut définir la multiplicité comme l'exposant de $X - \alpha$ dans la décomposition de P en facteurs irréductibles.

Définition III.B.3. Soit $P = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{K}[X]$ un polynôme. Son *polynôme dérivé* (ou encore sa *dérivée*) est le polynôme :

$$P' = a_1 + 2a_2 X + 3a_3 X^3 + \cdots + n a_n X^{n-1} \in \mathbb{K}[X].$$

Proposition III.B.4. L'opération de dérivation vérifie les propriétés habituelles de l'analyse : étant donné des polynômes $P, Q \in \mathbb{K}[X]$ et des scalaires $\alpha, \beta \in \mathbb{K}$, on a :

$$(\alpha P + \beta Q)' = \alpha P' + \beta Q', \qquad (PQ)' = P'Q + PQ', \qquad (P \circ Q)' = Q' \cdot (P' \circ Q).$$

Proposition III.B.5. Soit P un polynôme. Si une racine α de P est multiple alors $P'(\alpha) = 0$.

Démonstration. Si α est une racine multiple, alors $P = (X - \alpha)^2 \cdot Q$ avec $Q \in \mathbb{K}[X]$ et donc $P' = 2(X - \alpha)Q + (X - \alpha)^2 Q'$ s'annule bien en α.

Supposons maintenant que $P'(\alpha) = 0$. On peut écrire $P = (X - \alpha) \cdot R$ (car α est une racine) avec $R \in \mathbb{K}[X]$. La dérivée de P est donnée par $P' = (X - \alpha)R' + R$. Donc $P'(\alpha) = R(\alpha)$ est nul. Par division euclidienne, R est divisible par $X - \alpha$ et donc P est divisible par $(X - \alpha)^2$ comme attendu. ◇

§ III.B(a) Extensions algébriques

Définition III.B.6. Soit $\mathbb{K} \subset \mathbb{L}$ une extension de corps. On dit que l'extension est *algébrique* si tout élément de $\mathbb{L}$ est algébrique sur $\mathbb{K}$.

Corollaire III.B.7. Une extension finie est algébrique.

Démonstration. Si $\mathbb{K} \subset \mathbb{L}$ est une extension finie (c'est-à-dire $\dim_{\mathbb{K}} \mathbb{L} < \infty$) et si $\alpha \in \mathbb{L}$, alors :

$$\dim_{\mathbb{K}} \mathbb{K}[\alpha] \leq \dim_{\mathbb{K}} \mathbb{L} < \infty.$$ ◇

Exemple III.B.8. L'extension $\mathbb{R} \subset \mathbb{C}$ est algébrique. L'extension $\mathbb{Q} \subset \mathbb{R}$ ne l'est pas.

Théorème III.B.9. Soit $\mathbb{K} \subset \mathbb{L}$ une extension de corps. L'ensemble suivant est un corps :

$$\mathbb{K}' = \{ x \in \mathbb{L} \mid x \text{ est algébrique sur } \mathbb{K} \}.$$

C'est la plus grande extension algébrique de $\mathbb{K}$ contenue dans $\mathbb{L}$. On l'appelle[11] la *clôture algébrique de $\mathbb{K}$ dans $\mathbb{L}$*.

Il s'agit de montrer que $\mathbb{K}'$ est stable par addition, opposé, multiplication, et inverse. Cela n'a rien d'évident a priori.

Exercice III.B.10. Trouver les polynômes minimaux de $\sqrt{2} + \sqrt{3}$, puis de $\sqrt{2} + \sqrt{3} + \sqrt{5}$… Ou en tout cas, essayer !

Démonstration. Pour démontrer le théorème, nous allons employer les techniques vectorielles. Soit $x, y \in \mathbb{L}$ deux éléments algébriques sur $\mathbb{K}$, $y \neq 0$. Notre objectif est de démontrer que $x - y$ et x/y sont également algébriques sur $\mathbb{K}$.

Comme x est algébrique sur $\mathbb{K}$, $\mathbb{K}[x]$ est un corps et $[\mathbb{K}[x]: \mathbb{K}] < \infty$. De plus, y est algébrique sur $\mathbb{K}$, donc a fortiori sur $\mathbb{K}[x]$ et donc $\big[\mathbb{K}[x, y]: \mathbb{K}[x]\big] < \infty$. On en déduit donc, par multiplicativité du degré, que :

$$[\mathbb{K}[x, y]: \mathbb{K}] = \big[\mathbb{K}[x, y]: \mathbb{K}[x]\big] \cdot [\mathbb{K}[x]: \mathbb{K}] < \infty.$$

Or $x - y$ et x/y sont tous deux des éléments de $\mathbb{K}[x, y]$, donc $\mathbb{K}[x - y]$ et $\mathbb{K}[x/y]$ sont de dimensions finies sur $\mathbb{K}$ et donc $x - y$ et x/y sont tous deux algébriques. ◇

Exemple III.B.11. L'ensemble des nombres complexes algébriques sur $\mathbb{Q}$ forme un corps noté $\overline{\mathbb{Q}}$; c'est la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$. C'est une extension algébrique de $\mathbb{Q}$ qui n'est pas finie (car $\mathbb{Q}[X]$ contient des éléments irréductibles de degré arbitraires, cf. plus loin).

Introduisons maintenant une classe de corps qui n'ont pas d'extensions algébriques non triviales.

Définition III.B.12. Un polynôme $P \in \mathbb{K}[X]$ est *scindé* s'il se décompose en un produit (éventuellement vide) de facteurs de degré 1, éventuellement avec un facteur inversible.

Exemple III.B.13. Le polynôme $2X^2 - 3 = 2\left(X - \sqrt{3/2}\right)\left(X + \sqrt{3/2}\right)$ est scindé sur $\mathbb{R}$ mais pas sur $\mathbb{Q}$.

Définition III.B.14. Un corps $\mathbb{K}$ est *algébriquement clos* s'il satisfait les conditions équivalentes :

- Si $\mathbb{K} \subset \mathbb{L}$ est une extension algébrique, alors $\mathbb{K} = \mathbb{L}$.
- Tout polynôme de $\mathbb{K}[X]$ de degré ≥ 1 admet une racine.
- Tout polynôme de $\mathbb{K}[X]$ est scindé.
- Les éléments irréductibles de $\mathbb{K}[X]$ sont les polynômes de degré 1.

Exemple III.B.15. Le corps $\mathbb{C}$ est algébriquement clos (c'est le théorème fondamental de l'algèbre).

[11] À ne pas confondre avec la notion de « corps algébriquement clos » introduite plus loin !

Exercice III.B.16. Le corps $\overline{\mathbb{Q}}$ défini ci-dessus est algébriquement clos. Ce n'est pas évident au premier abord. En effet, tout polynôme à coefficients dans $\mathbb{Q}$ a une solution dans $\overline{\mathbb{Q}}$. Mais il faut démontrer que tout polynôme à coefficients dans $\overline{\mathbb{Q}}$ a encore une solution dans $\overline{\mathbb{Q}}$; en d'autres termes, si α est algébrique sur $\overline{\mathbb{Q}}$, alors il est déjà algébrique sur $\mathbb{Q}$.

Par exemple, supposons que $\alpha^3 + 2\alpha^2 - \alpha + 1 = 0$, et que $\beta^3 + \beta + 3 = 0$, donc α et β sont algébriques (mais irrationnels !). On suppose maintenant que γ est un nombre algébrique qui vérifie $\gamma^3 + \alpha\gamma^2 + \beta\gamma + 1 = 0$. Est-il facile de trouver un polynôme *à coefficients rationnels* qui s'annule en γ ? (Le polynôme minimal de γ est de degré $27 = 3^3$…)

La proposition suivante donne la solution.

Proposition III.B.17. Soit $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ des extensions, avec $\mathbb{L}$ algébrique sur $\mathbb{K}$ et $\mathbb{M}$ algébrique sur $\mathbb{L}$. Alors $\mathbb{M}$ est algébrique sur $\mathbb{K}$.

Démonstration. La preuve fait encore intervenir des techniques vectorielles. Soit $\alpha \in \mathbb{M}$ un élément. Comme $\mathbb{L} \subset \mathbb{M}$ est algébrique, il existe un polynôme $P = \beta_0 + \beta_1 X + \cdots + \beta_n X^n$ avec $\beta_i \in \mathbb{L}$ et $P(\alpha) = 0$. Chaque β_i est lui-même algébrique sur $\mathbb{K}$, donc $[\mathbb{K}[\beta_i]\colon \mathbb{K}] < \infty$. En réutilisant la preuve du **Théorème III.B.9**, on en déduit que :

$$[\mathbb{K}[\beta_1, \dots, \beta_n]\colon \mathbb{K}] < \infty.$$

Or α est algébrique sur $\mathbb{K}[\beta_1, \dots, \beta_n]$, donc $\left[\mathbb{K}[\beta_1, \dots, \beta_n, \alpha]\colon \mathbb{K}[\beta_1, \dots, \beta_n]\right] < \infty$. On déduit de ces deux inéquations que $[\mathbb{K}[\beta_1, \dots, \beta_n, \alpha]\colon \mathbb{K}] < \infty$, et comme $\alpha \in \mathbb{K}[\beta_1, \dots, \beta_n, \alpha]$, que $[\mathbb{K}[\alpha]\colon \mathbb{K}] < \infty$. On en déduit donc que α est bien algébrique sur $\mathbb{K}$. ◇

Nous allons démontrer plus loin que tout corps est contenu dans un corps algébriquement clos.

§ III.B(b) Corps de rupture

Notre objectif est maintenant de « forcer » un polynôme irréductible à avoir une racine.

Définition III.B.18. Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$ un polynôme irréductible. Un *corps de rupture* de P est une extension monogène $\mathbb{K} \subset \mathbb{K}(\alpha)$ telle que $P(\alpha) = 0$.

Remarque III.B.19. Le polynôme P est divisible par $X - \alpha$ dans $\mathbb{K}(\alpha)$ et n'y est donc plus irréductible s'il est de degré ≥ 2.

On rappelle qu'un $\mathbb{K}$-morphisme entre deux extensions est un morphisme de corps qui est l'identité sur le sous-corps $\mathbb{K}$.

Proposition III.B.20. Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$ un polynôme irréductible. Un corps de rupture de P existe et est unique à $\mathbb{K}$-isomorphisme près.

Démonstration. Pour l'existence, posons $\mathbb{L} = \mathbb{K}[X]/(P)$. Comme P est irréductible et $\mathbb{K}[X]$ est principal, l'idéal (P) est maximal, donc $\mathbb{L}$ est bien un corps. Si on pose $\alpha = [X] \in \mathbb{L}$, alors $P(\alpha) = 0$ et $\mathbb{L} = \mathbb{K}[\alpha] = \mathbb{K}(\alpha)$ est monogène.

Supposons maintenant que $\mathbb{L}' = \mathbb{K}(\alpha')$ est un (autre) corps de rupture de P. Il y a un unique morphisme de $\mathbb{K}$-algèbres $\varphi\colon \mathbb{K}[X] \to \mathbb{L}'$ tel que $\varphi(X) = \alpha'$; c'est l'évaluation en α'. Ce morphisme s'annule sur l'idéal (P) (car $P(\alpha') = 0$) donc φ factorise par $\mathbb{L} = \mathbb{K}[X]/(P) = \mathbb{K}[\alpha]$, avec $\varphi(\alpha) = \alpha'$. Ce morphisme factorisé est surjectif, car $\mathbb{L}'$ est monogène, engendré par α'. Il est de plus injectif :

comme P est irréductible, c'est le polynôme minimal (à inversible près) de α. C'est donc un $\mathbb{K}$-isomorphisme. ◇

On parlera donc en général du corps de rupture d'un polynôme plutôt que d'un corps de rupture.

Exemple III.B.21. Le corps $\mathbb{C}$ est le corps de rupture de X^2+1, car $\mathbb{C}=\mathbb{R}(i)$. C'est aussi le corps de rupture de X^2+X+1, car $\mathbb{C}=\mathbb{R}(j)$ avec $j=\exp(2i\pi/3)$. On remarque que dans $\mathbb{C}$, chacun de ces deux polynômes est scindé :

$$X^2+1=(X+i)(X-i), \qquad X^2+X+1=(X-j)(X-j^2).$$

Exemple III.B.22. Le corps $\mathbb{Q}(\sqrt[3]{2})$ est le corps de rupture de $P=X^3-2$. Le polynôme P est décomposable dans le corps de rupture :

$$X^3-2=\left(X-\sqrt[3]{2}\right)\left(X^2+\sqrt[3]{2}X+\sqrt[3]{4}\right).$$

Il n'est néanmoins pas scindé car $\mathbb{Q}(\sqrt[3]{2})$ ne contient pas ses autres racines, à savoir $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$.

Remarque III.B.23. On pourrait définir un « corps de rupture » d'un polynôme réductible $P\in\mathbb{K}[X]$ comme une extension monogène $\mathbb{K}(\alpha)$ telle que $P(\alpha)=0$. Cependant, on n'a pas unicité du corps de rupture dans ce cas. Par exemple, si $P=(X^2+1)(X^2-2)\in\mathbb{Q}[X]$, alors on a deux corps de rupture possibles à isomorphisme près, à savoir $\mathbb{Q}(i)$ et $\mathbb{Q}(\sqrt{2})$.

§ III.B(c) Corps de décomposition

Comme vu précédemment, même une fois qu'on a « forcé » un polynôme P à avoir une racine, il ne devient pas automatique scindé. Cela nous amène à considérer la définition suivante :

Définition III.B.24. Soit $\mathbb{K}$ un corps et $P\in\mathbb{K}[X]$ un polynôme. Un *corps de décomposition* de P est une extension $\mathbb{K}\subset\mathbb{L}$ telle que P est scindé dans $\mathbb{L}$ et qui est minimale pour cette propriété.

Théorème III.B.25. Soit $\mathbb{K}$ un corps et $P\in\mathbb{K}[X]$ un polynôme. Il existe un corps de décomposition de P, unique à $\mathbb{K}$-isomorphisme près.

Démonstration. L'existence se démontre par récurrence sur $\deg(P)$. Si $\deg(P)=0$ ou $\deg(P)=1$, alors $\mathbb{L}=\mathbb{K}$ convient et cette extension est bien sûr minimale. Supposons maintenant que tout polynôme de degré $<d$ admet un corps de décomposition (avec $d\geq 2$), et considérons P de degré d. Si P est déjà scindé, alors $\mathbb{L}=\mathbb{K}$ convient encore. Sinon, P admet un facteur irréductible de degré ≥ 2 (rappelons que $\mathbb{K}[X]$ est factoriel), disons $Q\in\mathbb{K}[X]$. Soit $\mathbb{K}'=\mathbb{K}(\alpha)$ le corps de rupture de Q. Alors dans $\mathbb{K}'[X]$, on a $P=(X-\alpha)\tilde{P}$ avec $\deg(\tilde{P})<d$. On peut donc considérer le corps de décomposition $\mathbb{L}$ de $\tilde{P}$, qui est une extension de $\mathbb{K}'$ et donc de $\mathbb{K}$. Cette extension est minimale, car engendrée par les racines $\alpha_2,\dots,\alpha_n\in\mathbb{K}[\alpha]$ (potentiellement multiples) de $\tilde{P}$ sur $\mathbb{K}[\alpha]$, et donc on a $\mathbb{L}=\mathbb{K}[\alpha,\alpha_2,\dots,\alpha_n]$.

Pour démontrer l'unicité, raisonnons par récurrence sur $[\mathbb{L}:\mathbb{K}]$. Si le degré de l'extension vaut 1, alors $\mathbb{L}=\mathbb{K}$ est bien sûr unique. Supposons maintenant que si un polynôme quelconque admet un corps de décomposition de degré $<d$ sur $\mathbb{K}$ (avec $d\geq 2$), alors tout autre corps de décomposition de ce polynôme lui est $\mathbb{K}$-isomorphe. Supposons que P admet un corps de décomposition de degré $[\mathbb{L}:\mathbb{K}]=d$ et soit $\mathbb{L}'$ un autre corps de décomposition. Soit $\alpha\in\mathbb{L}\setminus\mathbb{K}$ une racine de P, et soit $Q\in\mathbb{K}[X]$ le polynôme minimal de α. Le polynôme Q est un facteur irréductible de P, et il admet donc une racine $\alpha'\in\mathbb{L}'\setminus\mathbb{K}$. Si l'on note $\mathbb{M}=\mathbb{K}(\alpha)\subset\mathbb{L}$ et $\mathbb{M}'=\mathbb{K}(\alpha')\subset\mathbb{L}'$, ces deux corps sont des corps de rupture de P et donc il existe un $\mathbb{K}$-isomorphisme $f:\mathbb{M}\to\mathbb{M}'$ tel que $\varphi(\alpha)=\alpha'$. Mais alors $\mathbb{M}\subset\mathbb{L}$ et $\mathbb{M}(\subset\mathbb{M}')\subset\mathbb{L}'$ sont deux corps de rupture de P de degré $<d$ sur $\mathbb{M}$, donc on peut appliquer l'hypothèse de

récurrence et trouver un $\mathbb{M}$-isomorphisme ψ entre eux. Comme $\varphi\colon \mathbb{M} \to \mathbb{M}'$ était un $\mathbb{K}$-isomorphisme, ψ se restreint bien en l'identité sur $\mathbb{K}$ et on peut conclure. ◇

Définition III.B.26. Étant donné $P \in \mathbb{K}[X]$, on notera $\mathcal{D}_{\mathbb{K}}(P)$ sont corps de décomposition sur $\mathbb{K}$.

Remarque III.B.27. En suivant la preuve, on voit que $\mathcal{D}_{\mathbb{K}}(P)$ est engendré par les racines de P.

Exemple III.B.28. Le corps $\mathbb{C}$ est le corps de décomposition de $X^2 + 1$ sur $\mathbb{R}$. On note qu'ici, le corps de rupture est déjà un corps de décomposition ; ce n'est pas toujours le cas.

Exemple III.B.29. Le corps $\mathbb{Q}\left(j, \sqrt[3]{2}\right)$ est le corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$.

§ III.B(d) Clôture algébrique

Enfin, nous allons étudier une manière de « forcer » *tous* les polynômes à être scindés.

Théorème III.B.30 (Steinitz). Soit $\mathbb{K}$ un corps. Il existe une extension de $\mathbb{K}$ qui :

- Est algébrique sur $\mathbb{K}$;
- Est algébriquement close, c.-à-d., tout polynôme y est scindé.

Cette extension est unique à $\mathbb{K}$-isomorphisme près et on l'appelle la *clôture algébrique* de $\mathbb{K}$.

Exemple III.B.31. Le corps $\mathbb{C}$ est la clôture algébrique de $\mathbb{R}$.

Exemple III.B.32. Le corps $\overline{\mathbb{Q}}$ introduit précédemment est la clôture algébrique de $\mathbb{Q}$.

Pour démontrer le théorème, nous aurons besoin de quelques lemmes.

Lemme III.B.33. Soit $\mathbb{K}$ un corps et $P_1, \dots, P_r$ des polynômes. Il existe une extension finie $\mathbb{K} \subset \mathbb{L}$ telle que chaque polynôme P_i a une racine dans $\mathbb{L}$.

Démonstration. Il suffit de calculer plusieurs fois de suite les corps de rupture : on considère $\mathbb{L}_1$ le corps de rupture de P_1, puis $\mathbb{L}_2$ le corps de rupture de $P_2 \in \mathbb{K}[X] \subset \mathbb{L}_1[X]$, et ainsi de suite jusqu'à $\mathbb{L} = \mathbb{L}_r$. ◇

Lemme III.B.34. Soit $\mathbb{K}$ un corps. Il existe une extension $\mathbb{K} \subset \mathbb{K}'$ telle que tout polynôme de degré ≥ 1 à coefficients dans $\mathbb{K}$ a une racine dans $\mathbb{K}'$.

Remarque III.B.35. L'extension en question n'est pas nécessairement la clôture algébrique de $\mathbb{K}$, car il faudrait que tous les polynômes à coefficients dans $\mathbb{K}'$ aient une racine dans $\mathbb{K}'$, ce qui n'est pas forcément le cas.

Démonstration. Étant donné un polynôme $P \in \mathbb{K}[X]$ de degré ≥ 1, on définit une variable formelle X_P et on note $\mathcal{S}$ l'ensemble des variables X_P. On considère maintenant l'anneau $\mathbb{K}[\mathcal{S}]$ des polynômes en les variables X_P. Nous allons montrer que l'idéal suivant est non-trivial :

$$I = \left(P(X_P) \mid P \in \mathbb{K}[X], \deg(P) \geq 1 \right) \subset \mathbb{K}[\mathcal{S}].$$

L'idéal I n'est évidemment pas nul. Démontrons qu'il n'est pas égal à $\mathbb{K}[\mathcal{S}]$. Si au contraire il l'était, il existerait des polynômes $P_1, \dots, P_r \in \mathbb{K}[X]$ et des polynômes $Q_1, \dots, Q_r \in \mathbb{K}[\mathcal{S}]$ tels que :

$$Q_1 P_1\left(X_{P_1}\right) + \cdots + Q_r P_r\left(X_{P_r}\right) = 1. \qquad (*)$$

Soit $\mathbb{M}$ une extension finie de $\mathbb{K}$ dans laquelle chaque P_i a une racine $\alpha_i \in \mathbb{M}$. L'équation $(*)$ est encore valable à coefficients dans $\mathbb{M}$. Elle ne fait intervenir qu'un nombre fini de variables : les X_{P_i} et

les autres variables $X_{\dots} \in \mathcal{S}$ qui interviennent dans les Q_i. En évaluant l'équation $(*)$ sur $X_{P_i} = \alpha_i$ (et $X_{\dots} = 0$ pour les autres variables qui apparaissent), on obtient $0 = 1$ dans $\mathbb{M}$, une contradiction. Donc I est strictement inclus dans $\mathbb{K}[\mathcal{S}]$.

D'après le théorème de Krull (**Théorème II.B.20**), il existe un idéal maximal $\mathfrak{m}$ tel que $I \subset \mathfrak{m} \subsetneq \mathbb{K}[\mathcal{S}]$. Le quotient $\mathbb{L} \coloneqq \mathbb{K}[\mathcal{S}]/\mathfrak{m}$ est une extension de $\mathbb{K}$, et chaque polynôme $P \in \mathbb{K}[X]$ admet la racine X_P dans cette extension. ◇

Lemme III.B.36. Tout corps est contenu dans un corps algébriquement clos.

Remarque III.B.37. Il ne s'agit pas nécessairement de la clôture algébrique du corps, car on n'a pas supposé que l'extension soit algébrique sur le corps initial.

Démonstration. Soit $\mathbb{K}$ un corps. En utilisant le lemme précédent, on peut construire une suite d'extensions :

$$\mathbb{K} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \mathbb{K}_2 \subset \cdots$$

Qui vérifie la propriété suivante : tout polynôme à coefficients dans $\mathbb{K}_n$ de degré ≥ 1 admet une racine dans $\mathbb{K}_{n+1}$. Notons $\mathbb{L}$ la réunion des $\mathbb{K}_n$, qui forme un corps. Si $P \in \mathbb{L}[X]$ est un polynôme, tous ses coefficients sont dans l'un des $\mathbb{K}_n$ (pour n assez grand), donc P admet une racine dans $\mathbb{K}_{n+1}$ et donc dans le corps $\mathbb{L}$. ◇

Nous pouvons maintenant démontrer la partie « existence » du théorème. Soit $\mathbb{K}$ un corps et $\mathbb{K} \subset \mathbb{L}$ une extension avec $\mathbb{L}$ algébriquement close (obtenue par le lemme précédent). On note :

$$\overline{\mathbb{K}} \coloneqq \bigcup \{ \mathbb{M} \mid \mathbb{K} \subset \mathbb{M} \subset \mathbb{L},\ \mathbb{M} \text{ est algébrique sur } \mathbb{K} \}.$$

Alors $\overline{\mathbb{K}}$ est une extension algébrique de $\mathbb{K}$. De plus, si $P \in \overline{\mathbb{K}}[X]$ est un polynôme de degré ≥ 1, il admet une racine $\alpha \in \mathbb{L}$. Cet élément α est algébrique sur $\overline{\mathbb{K}}$, et $\overline{\mathbb{K}}$ est algébrique sur $\mathbb{K}$, donc α est algébrique sur $\mathbb{K}$ par la **Proposition III.B.17**, et donc finalement $\alpha \in \overline{\mathbb{K}}$.

Pour démontrer l'unicité, nous aurons besoin de quelques résultats supplémentaires sur les prolongements de morphismes vers des corps algébriquement clos.

Proposition III.B.38. Soit $\varphi\colon \mathbb{K} \hookrightarrow \mathbb{L}$ une extension de $\mathbb{K}$ dans un corps algébriquement clos. Soit $\mathbb{K}(\alpha)$ une extension algébrique monogène (non triviale) de $\mathbb{K}$, avec $P \in \mathbb{K}[X]$ le polynôme minimal de α qui possède r racines *distinctes* dans $\mathbb{L}$. Il y a exactement r prolongements $\varphi'\colon \mathbb{K}(\alpha) \to \mathbb{L}$ de φ en un $\mathbb{K}$-morphisme.

Démonstration. Notons que tout élément $y \in \mathbb{K}(\alpha)$ est de la forme $y = Q(\alpha)$ pour $Q \in \mathbb{K}[X]$. Pour chaque racine $\beta \in \mathbb{L}$ de P, on définit un prolongement $\varphi'\colon \mathbb{K}(\alpha) \to \mathbb{L}$ en posant :

$$\varphi'(y) \coloneqq Q(\beta).$$

Cet élément ne dépend pas du choix de Q : si $y = Q(\alpha) = R(\alpha)$, alors $(Q - R)(\alpha) = 0$ et donc P divise $Q - R$, donc $Q(\beta) - R(\beta) = 0$. Il n'est pas difficile de vérifier que φ' définit un $\mathbb{K}$-morphisme, que tous les $\mathbb{K}$ -morphismes sont de cette forme, et que des racines distinctes de μ donnent des prolongements distincts. ◇

Remarque III.B.39. Le nombre de racines distinctes de P n'est pas toujours égal au degré de P. Les contre-exemples ne se manifestent cependant qu'en caractéristique non-nulle. Nous verrons dans le Chapitre V que la proposition précédente et cette remarque entraînent des conséquences profondes.

Corollaire III.B.40. Soit $\mathbb{K}$ un corps, $\mathbb{K}'$ une extension algébrique de $\mathbb{K}$, et $\mathbb{L}$ une extension algébriquement close de $\mathbb{K}$. Il existe un $\mathbb{K}$-morphisme $\varphi: \mathbb{K}' \to \mathbb{L}$ qui prolonge $\mathbb{K} \subset \mathbb{L}$. Si de plus $\mathbb{K}'$ est algébriquement clos et si $\mathbb{L}$ est une extension algébrique de $\mathbb{K}$, alors φ est un $\mathbb{K}$-isomorphisme.

Démonstration. Pour démontrer ce corollaire, il faut faire appel à la proposition précédente et à l'axiome du choix, voir par exemple [6, Théorème 5.2.8]. La partie « unicité » du théorème découle immédiatement de ce corollaire. ◇

Section III.C. Exemples

§ III.C(a) Clôture algébrique de $\mathbb{Q}$

On rappelle que la clôture algébrique de $\mathbb{Q}$ est l'ensemble $\overline{\mathbb{Q}}$ défini précédemment :

$$\overline{\mathbb{Q}} \coloneqq \{ x \in \mathbb{C} \mid \exists P \in \mathbb{Q}[X],\ P(x) = 0 \}.$$

Donnons quelques propriétés de cet ensemble.

Proposition III.C.1. L'extension $\mathbb{Q} \subset \overline{\mathbb{Q}}$ est infinie.

Démonstration. Il suffit de montrer qu'il existe des polynômes à coefficients rationnels irréductibles de degré arbitrairement grands. En effet, si P est un tel polynôme et $\alpha \in \overline{\mathbb{Q}}$ en est une racine, alors l'extension $\mathbb{Q}(\alpha) \subset \overline{\mathbb{Q}}$ est de dimension $\deg(P)$. On peut utiliser le critère d'Eisenstein (**Théorème II.E.11**) : si p est un nombre premier, et $n \geq 1$ est un entier, alors $X^n - p$ est irréductible. Ce résultat entraîne que la famille $\{p, \sqrt{p}, \sqrt[3]{p}, \sqrt[4]{p} \dots\}$ est $\mathbb{Q}$-linéairement indépendante. ◇

Malgré cela, l'extension $\mathbb{Q} \subset \overline{\mathbb{Q}}$ reste de taille « raisonnable » :

Proposition III.C.2. Le corps $\overline{\mathbb{Q}}$ est dénombrable.

Démonstration. Pour $d \in \mathbb{N}$, on note $\mathbb{Q}_d[X]$ l'ensemble des polynômes de degré d à coefficients rationnels. On a alors :

$$\overline{\mathbb{Q}} = \bigcup_{d \in \mathbb{N}} \bigcup_{P \in \mathbb{Q}_d[X]} P^{-1}(\{0\}).$$

Pour chaque $P \in \mathbb{Q}_d[X]$, l'ensemble $P^{-1}(\{0\}) = \{ x \in \mathbb{Q} \mid P(x) = 0 \}$ est fini, de cardinal $\leq d$. De plus, l'ensemble $\mathbb{Q}_d[X]$ est dénombrable, car en bijection avec $\mathbb{Q}^* \times \mathbb{Q}^d$. Une réunion dénombrable d'ensembles dénombrables est dénombrable, donc $\bigcup_{P \in \mathbb{Q}_d[X]} P^{-1}(\{0\})$ est dénombrable. Comme $\mathbb{N}$ est encore dénombrable, on en déduit le résultat. ◇

Remarque III.C.3. La même preuve permet de démontrer que si $\mathbb{K}$ est infini, alors $\overline{\mathbb{K}}$ a le même cardinal que $\mathbb{K}$.

Corollaire III.C.4. Il existe des nombres réels transcendants.

Démonstration. Le corps $\mathbb{C}$ n'est pas dénombrable[12] mais $\overline{\mathbb{Q}}$ l'est, donc $\overline{\mathbb{Q}}$ est strictement contenu dans $\mathbb{C}$. ◇

[12] On peut le démontrer avec l'argument diagonal de Cantor. Restreignons-nous à $[0, 1]$ pour plus de simplicité. Imaginons que $\{x_n\}_{n \geq 0}$ est une énumération de tous les réels entre 0 et 1. On écrit en base décimale (sous forme normalisée, sans suite infinie de 9 à la fin) :

Ce résultat ne nous dit pas comment trouver un nombre transcendant ! Le premier nombre dont on a démontré qu'il était transcendant était la constante de Liouville.

Définition III.C.5. La constante de Liouville L est le nombre défini par :

$$\mathcal{L} := \sum_{n\geq 1} 10^{-n!}.$$

En base 10, ce nombre s'écrit $0{,}11000100000000000000000010\ldots$: toutes ses décimales sont nulles, sauf celles aux rangs de la forme $n!$ $(1, 2, 6, 24\ldots)$ qui valent 1.

Théorème III.C.6 (Liouville). Le nombre $\mathcal{L}$ est transcendant.

Cela découle des deux résultats suivants (que nous n'allons pas démontrer) :

Lemme III.C.7. Pour tout $n \geq 1$, il existe un irrationnel $p/q \in \mathbb{Q}$, $q > 1$, tel que :

$$0 < \left|\mathcal{L} - \frac{p}{q}\right| < \frac{1}{q^n}.$$

Ce lemme dit que $\mathcal{L}$ est approchable « aussi près que l'on veut » par un rationnel.

Lemme III.C.8. Soit α un nombre irrationel et n le degré de son polynôme minimal. Alors il existe une constante réelle $C > 0$ telle que pour tout $p/q \in \mathbb{Q}$,

$$\left|\alpha - \frac{p}{q}\right| > \frac{C}{q^n}.$$

Ce lemme dit au contraire qu'un nombre algébrique irrationnel n'est *pas* approchable par des nombres rationnels avec une précision arbitraire.

§ III.C(b) Construction à la règle et au compas

Dans cette section, nous allons donner une jolie application de la notion d'algébricité.

Définition III.C.9. Soit $A \subset \mathbb{R}^2$ un sous-ensemble du plan. On dit qu'un point est *constructible (à la règle et au compas) en un pas à partir de* A si on peut l'obtenir à partir de A en réalisant l'une des trois opérations suivantes :

- Prendre l'intersection de deux droites non-parallèles passant chacune par deux points de A ;
- Prendre un point d'intersection d'une droite passant par deux points de A avec un cercle dont le centre est dans A et qui passe par un autre point de A ;
- Prendre un point d'intersection entre deux cercles distincts, dont chacun des centres est dans A et chacun passe par un point de A.

On dit qu'un point P est *constructible à partir de* A s'il existe une suite $A = A_0 \subset A_1 \subset \cdots \subset A_n$ telle que pour tout k, $A_{k+1} = A_k \cup \{P_k\}$ avec P_k constructible en un pas à partir de A_k et $P = P_n$.

On dit aussi que P est *constructible* (tout court) s'il est constructible à partir de $A = \{(0,0),(1,0)\}$. Enfin, on dit qu'un nombre réel $x \in \mathbb{R}$ est *constructible* si $(x, 0)$ est constructible.

$$x_n = 0, x_n^0 x_n^1 x_n^2 \ldots$$

On construit alors le nombre α dont la $k$ième décimale est $x_k^k + 1 \pmod{10}$. Par construction, ce nombre ne peut pas apparaître dans la liste $\{x_n\}$: s'il était égal à x_n, leurs $n$ième décimales seraient égales !

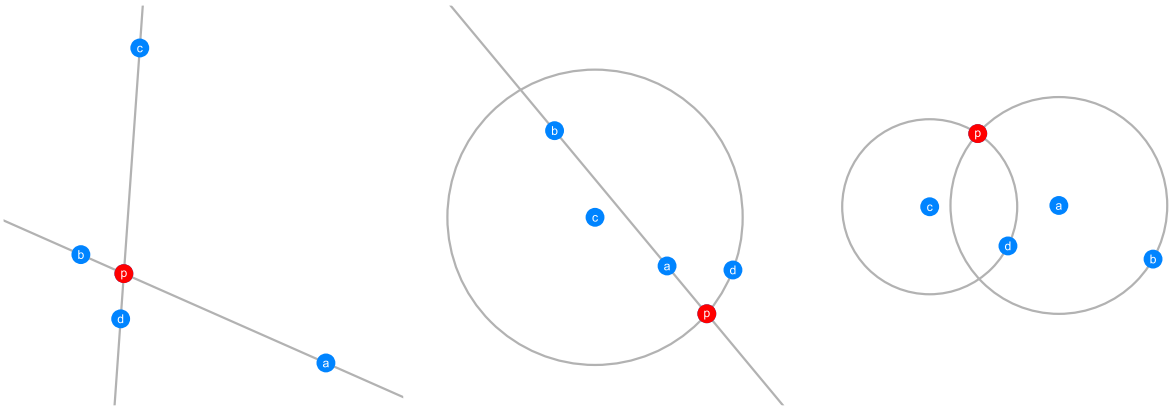


Figure III.C-a Les trois manières de construire des points, de gauche à droite : intersection de deux droites, intersection d'une droite et d'un cercle, intersection de deux cercles.

Exercice III.C.10. On dit qu'une droite (resp., un cercle) est constructible si elle passe par deux points constructibles (resp., son centre est constructible et il passe par un point constructible). Démontrer que :

- Si $\mathcal{D}$ est une droite constructible, et $P \notin \mathcal{D}$ est un point constructible, alors la parallèle à $\mathcal{D}$ et la perpendiculaire à $\mathcal{D}$ qui passent par P sont constructibles.
- Si P, Q, R sont constructibles, alors le cercle de centre P et de rayon $\|\overrightarrow{QR}\|$ est constructible.

Exercice III.C.11. Soit $n \in \mathbb{Z}$ un entier. Démontrer que $(n, 0)$ et $(0, n)$ sont constructibles.

Exercice III.C.12. Soit $x \in \mathbb{Q}$ un rationnel. Démontrer que x est constructible. (Indice : utiliser le théorème de Thalès.)

Exercice III.C.13. Soit x un réel constructible. Démontrer que $\sqrt{x}$ est constructible. (Indice : utiliser le théorème de Pythagore.)

Passons maintenant au lien entre nombres constructibles et algèbre.

Proposition III.C.14. Si x est un réel constructible, alors le degré de l'extension $[\mathbb{Q}(x) : \mathbb{Q}]$ est une puissance de deux.

Comme dans la définition, posons $A_0 = \{(0,0),(1,0)\} \subset A_1 \subset \cdots \subset A_n$ avec $A_{i+1} = A_i \cup \{P_i\}$, P_{i+1} constructible en un pas à partir de A_i, et $P_n = (x, 0)$. On note $\mathbb{K}_i$ l'extension de $\mathbb{Q}$ engendrée par les coordonnées des points de A_i, de telle sorte que l'on a une tour d'extensions :

$$\mathbb{Q} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_n \ni x.$$

Lemme III.C.15. Quel que soit i, le degré $[\mathbb{K}_{i+1} : \mathbb{K}_i]$ vaut 1, 2 ou 4.

Démonstration. Le point $P_{i+1} = (x_{i+1}, y_{i+1})$ est défini par l'intersection de droites et/ou de cercles et on a $\mathbb{K}_{i+1} = \mathbb{K}_i(x_{i+1}, y_{i+1})$.. L'équation d'une droite est de degré 1 et l'équation de cercles de degré 2, donc on a $[\mathbb{K}_i(x_{i+1}) : \mathbb{K}_i] \in \{1, 2\}$ et de même $[\mathbb{K}_i(y_{i+1}) : \mathbb{K}_i] \in \{1, 2\}$, donc le degré cherché, $[\mathbb{K}_i(x_{i+1}, y_{i+1}) : \mathbb{K}_i] = [\mathbb{K}_i(x_{i+1}, y_{i+1}) : \mathbb{K}_i(x_{i+1})] \cdot [\mathbb{K}_i(x_{i+1}) : \mathbb{K}_i]$, vaut 1, 2 ou 4. ◇

Exercice III.C.16. Démontrer qu'en fait, le degré vaut toujours 1 ou 2. (Indice : décrire l'intersection de deux cercles comme l'intersection d'un cercle et d'une droite.)

Démonstration. Ce lemme permet de démontrer la proposition : le degré $[\mathbb{K}_n : \mathbb{Q}]$ est un produit de facteurs tous égaux à 1, 2 ou 4, donc c'est une puissance de 2. Par multiplicativité du degré, $[\mathbb{Q}(x) : \mathbb{Q}]$ divise $[\mathbb{K}_n : \mathbb{Q}]$, d'où le résultat. ◇

Cela permet de résoudre plusieurs problèmes posés par les géomètres de la Grèce antique :

- La duplication du cube : peut-on construire (à la règle et au compas) un cube de volume double du volume du cube unité ? En d'autres termes, est-ce que $\sqrt[3]{2}$ est constructible à la règle et au compas ?
- La trisection de l'angle : peut-on couper en trois angles égaux (« trissecter ») l'angle d'un triangle équilatéral ? En d'autres termes, peut-on construire $\cos(\pi/9)$? (La construction de la bissectrice à la règle et au compas est bien connue !)
- La quadrature du cercle : peut-on construire un carré de même aire que le cercle unité ? En d'autres termes, peut-on construire $\sqrt{\pi}$?

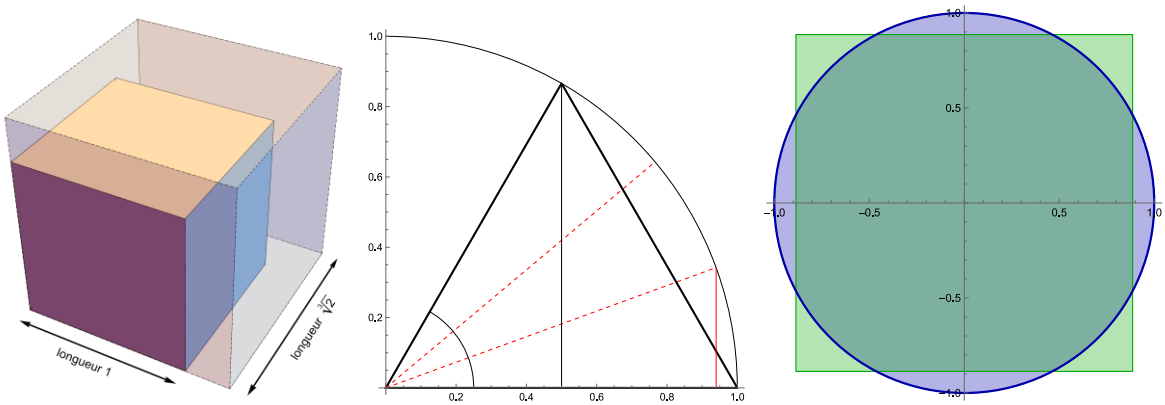


Figure III.C-b Les trois problèmes classiques : duplication du cube, trisection de l'angle, quadrature du cercle.

Corollaire III.C.17. La duplication du cube est impossible : $\sqrt[3]{2}$ n'est pas constructible.

Démonstration. Son polynôme minimal est $X^3 - 2$ et donc $\left[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}\right]$ vaut 3, qui n'est pas une puissance de deux. ◇

Corollaire III.C.18. La trisection de l'angle est impossible : $\cos(\pi/9)$ n'est pas constructible.

Démonstration. On a l'équation $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$ qui donne dans notre cas, pour $\theta = \pi/9$,

$$4\alpha^3 - 3\alpha = \cos(\pi/3) = 1/2 \Leftrightarrow 8\alpha^3 - 6\alpha - 1 = 0.$$

On vérifie que $P = 8X^3 - 3X - 1$ est irréductible (les racines rationnelles éventuelles sont à chercher parmi $\{\pm 1, \pm 1/2, \pm 1/4, \pm 1/8\}$ mais aucune ne marche). C'est donc le polynôme minimal de α et $[\mathbb{Q}(\alpha):\mathbb{Q}] = 3$, qui n'est pas une puissance de deux. Donc α n'est pas constructible. ◇

Pour la quadrature du cercle, la preuve utilise le théorème suivant (que nous n'allons pas démontrer) :

Théorème III.C.19 (Lindemann). Le nombre π est transcendant.

Corollaire III.C.20. La quadrature de cercle est impossible : $\sqrt{\pi}$ n'est pas constructible.

Démonstration. Si $\sqrt{\pi}$ était constructible, il serait algébrique, et son carré $\pi = \sqrt{\pi} \cdot \sqrt{\pi}$ le serait aussi. Or ce n'est pas le cas d'après le théorème de Lindemann. ◇

Remarque III.C.21. Les origamis permettent de construire plus de nombres que la règle et le compas : ils permettent de construire toutes les tours d'extensions dont les étages intermédiaires sont de degré 2 ou 3 (voir [4, chapitre 3]). Ils permettent donc de dupliquer le cube et trissecter le triangle équilatéral. Mais pas de réaliser la quadrature du cercle, qui reste inaccessible aux méthodes algébriques…

§ III.C(c) Quelques exemples en caractéristique non-nulle

En caractéristique nulle, on « triche » un peu quand il s'agit d'étudier les extensions algébriques de $\mathbb{Q}$. En effet, on connaît déjà l'extension $\mathbb{C}$ dont on sait qu'elle est algébriquement close (la preuve faisant intervenir de l'analyse). Grâce aux résultats des sections précédentes, n'importe quelle extension algébrique de $\mathbb{Q}$ se plonge dans $\mathbb{C}$, et on peut compter et déterminer les plongements possibles d'une extension finie explicitement. La connaissance de $\mathbb{C}$ permet par ailleurs de définir facilement[13] la clôture algébrique $\overline{\mathbb{Q}}$ de $\mathbb{Q}$.

La situation est différente en caractéristique $p > 0$ (premier). On ne connaît a priori qu'un seul corps de caractéristique p, le corps $\mathbb{Z}/p\mathbb{Z}$, et ses extensions évidentes comme le corps des fractions rationnelles $\mathbb{Z}/p\mathbb{Z}(X)$. On ne connaît pas d'extension algébriquement close de $\mathbb{Z}/p\mathbb{Z}$. Plusieurs arguments qui s'appliquent à $\mathbb{Q} = K_{\mathbb{Z}}$ (le critère d'Eisenstein, par exemple) ne s'appliquent pas à $\mathbb{Z}/p\mathbb{Z}$.

Nous allons donner ici quelques exemples d'extensions algébriques de $\mathbb{Z}/p\mathbb{Z}$ pour quelques valeurs de p. On étudiera plus en détail les corps finis dans le Chapitre IV.

Exemple III.C.22. Le polynôme $X^2 + X + 1$ est le seul polynôme irréductible de degré 2 à coefficients dans $\mathbb{Z}/2\mathbb{Z}$. En effet, on vérifie qu'il n'a pas de racines, et tous les autres polynômes de degré 2 (il y en a trois) ont une racine.

Son corps de rupture $\mathbb{K} = \mathbb{Z}/2\mathbb{Z}[X]/(X^2 + X + 1) = \mathbb{Z}/2\mathbb{Z}[\alpha]$ est la seule extension quadratique. L'élément α vérifie l'équation $\alpha^2 + \alpha + 1 = 0$ (ou encore $\alpha^2 = \alpha + 1$). Son cardinal vaut $|\mathbb{Z}/2\mathbb{Z}|^2 = 2^2 = 4$. Attention, il n'est pas isomorphe à l'anneau $\mathbb{Z}/4\mathbb{Z}$, qui n'est pas un corps ! Tous ses éléments $x \in \mathbb{K}$ vérifient $2x = x + x = 0$, ce qui n'est pas le cas dans $\mathbb{Z}/4\mathbb{Z}$. Ses éléments sont $\{0, 1, \alpha, \alpha + 1\}$ (les classes des quatre polynômes de degré < 2 à coefficients dans $\mathbb{Z}/2\mathbb{Z}$). Sa table de multiplication est la suivante :

$\times$	$\mathbf{0}$	$\mathbf{1}$	$\boldsymbol{\alpha}$	$\boldsymbol{\alpha+1}$
$\mathbf{0}$	0	0	0	0
$\mathbf{1}$	0	1	α	$\alpha+1$
$\boldsymbol{\alpha}$	0	α	$\alpha+1$	1
$\boldsymbol{\alpha+1}$	0	$\alpha+1$	1	α

Exemple III.C.23. Il y a deux polynômes irréductibles de degré 3 sur $\mathbb{Z}/2\mathbb{Z}$, à savoir $Q = X^3 + X + 1$ et $R = X^3 + X^2 + 1$. Ces deux polynômes définissent deux extensions :

$$\mathbb{L} = \mathbb{Z}/2\mathbb{Z}[X]/(Q) = \mathbb{Z}/2\mathbb{Z}[\beta], \qquad \mathbb{M} = \mathbb{Z}/2\mathbb{Z}[X]/(R) = \mathbb{Z}/2\mathbb{Z}[\gamma].$$

Chacune de ces extensions est de cardinal 8. En tant que $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel, des bases sont données par $\{1, \beta, \beta^2\}$ et $\{1, \gamma, \gamma^2\}$. Les éléments β et γ vérifient respectivement les équations $\beta^3 = \beta + 1$ et $\gamma^3 = \gamma^2 + 1$, à partir desquelles on peut trouver les tables de multiplication de $\mathbb{K}$ et $\mathbb{L}$ (de taille $8^2 = 64$, non reproduites ici).

En fait, ces deux extensions sont $\mathbb{Z}/2\mathbb{Z}$-isomorphes. On peut définir un isomorphisme :

$$\varphi\colon \mathbb{K} \to \mathbb{L}, \qquad \beta \mapsto \varphi(\beta) = \gamma + 1.$$

[13] Cette facilité n'est qu'apparente ! On ne sait, somme toute, pas grand-chose sur $\overline{\mathbb{Q}}$…

En effet, l'élément $\gamma+1$ vérifie bien l'équation $(\gamma+1)^3=\gamma=(\gamma+1)+1$, donc le morphisme d'anneaux $\mathbb{Z}/2\mathbb{Z}[X]\to\mathbb{M}$, $X\mapsto\gamma+1$ factorise bien par $\mathbb{L}$. Il est clairement surjectif, donc comme $|\mathbb{M}|=|\mathbb{L}|$, c'est un isomorphisme. Il n'y a donc qu'une unique extension cubique de $\mathbb{Z}/2\mathbb{Z}$.

On remarque également que l'extension quadratique $\mathbb{K}=\mathbb{Z}/2\mathbb{Z}[\alpha]$ trouvée précédemment **ne** se plonge **pas** dans $\mathbb{L}=\mathbb{M}$. En effet, l'équation $X^2=X+1$ qui définit α n'admet pas de solution dans $\mathbb{L}$: si on pose $x=x_0+x_1\beta+x_2\beta^2$ (avec $x_i\in\{0,1\}$), alors on a :

$$\begin{aligned}x^2&=(x_0+x_1\beta+x_2\beta^2)^2\\&=x_0+x_1\beta^2+x_2\beta^4\\&=x_0+x_1\beta^2+x_2\beta(\beta+1)\\&=x_0+x_2\beta+(x_1+x_2)\beta^2.\end{aligned}$$

Pour avoir $x^2=x+1$, il faudrait donc avoir $x_0=x_0+1$, ce qui est impossible.

En degré supérieur, il est plus difficile de chercher les polynômes irréductibles. On peut vérifier par exemple qu'il y a quatre polynômes de degré 4 qui n'ont pas de racines : $1+X^3+X^4$, $1+X^2+X^4$, $1+X+X^4$, et $1+X+X^2+X^3+X^4$. Cependant, ils ne sont pas tous irréductibles : le polynôme X^4+X^2+1 se décompose en fait comme $(X^2+X+1)^2$. Les trois autres sont irréductibles et définissent des extensions quartiques de $\mathbb{Z}/2\mathbb{Z}$, dont on peut vérifier (c'est laborieux) qu'elles sont isomorphes.

Exemple III.C.24. Il y a trois polynômes irréductibles de degré 2 sur $\mathbb{Z}/3\mathbb{Z}$, à savoir $P=X^2+1$, $Q=X^2+X+2$ et $R=X^2+2X+2$. Ils définissent chacun une extension monogène quadratique,

$$\mathbb{K}=\mathbb{Z}/3\mathbb{Z}[\alpha],\qquad \mathbb{L}=\mathbb{Z}/3\mathbb{Z}[\beta],\qquad \mathbb{M}=\mathbb{Z}/3\mathbb{Z}[\gamma].$$

Chacune de ces extensions est de cardinal $3^2=9$, avec $\mathbb{K}=\{0,1,2,\alpha,\alpha+1,\alpha+2,2\alpha,2\alpha+1,2\alpha+2\}$ (et de même pour $\mathbb{L}$ et $\mathbb{M}$). Les générateurs vérifient respectivement $\alpha^2=2$, $\beta^2=2\beta+1$ et $\gamma^2=\gamma+1$, ce qui permet de trouver les tables de multiplication. Pour $\mathbb{K}$, on trouve par exemple la table suivante :

$\times$	$\mathbf{0}$	$\boldsymbol{\alpha}$	$\mathbf{2}\,\boldsymbol{\alpha}$	$\mathbf{1}$	$\mathbf{1}+\boldsymbol{\alpha}$	$\mathbf{1}+\mathbf{2}\,\boldsymbol{\alpha}$	$\mathbf{2}$	$\mathbf{2}+\boldsymbol{\alpha}$	$\mathbf{2}+\mathbf{2}\,\boldsymbol{\alpha}$
$\mathbf{0}$	0	0	0	0	0	0	0	0	0
$\boldsymbol{\alpha}$	0	2	1	α	$2+\alpha$	$1+\alpha$	$2\,\alpha$	$2+2\,\alpha$	$1+2\,\alpha$
$\mathbf{2}\,\boldsymbol{\alpha}$	0	1	2	$2\,\alpha$	$1+2\,\alpha$	$2+2\,\alpha$	α	$1+\alpha$	$2+\alpha$
$\mathbf{1}$	0	α	$2\,\alpha$	1	$1+\alpha$	$1+2\,\alpha$	2	$2+\alpha$	$2+2\,\alpha$
$\mathbf{1}+\boldsymbol{\alpha}$	0	$2+\alpha$	$1+2\,\alpha$	$1+\alpha$	$2\,\alpha$	2	$2+2\,\alpha$	1	α
$\mathbf{1}+\mathbf{2}\,\boldsymbol{\alpha}$	0	$1+\alpha$	$2+2\,\alpha$	$1+2\,\alpha$	2	α	$2+\alpha$	$2\,\alpha$	1
$\mathbf{2}$	0	$2\,\alpha$	α	2	$2+2\,\alpha$	$2+\alpha$	1	$1+2\,\alpha$	$1+\alpha$
$\mathbf{2}+\boldsymbol{\alpha}$	0	$2+2\,\alpha$	$1+\alpha$	$2+\alpha$	1	$2\,\alpha$	$1+2\,\alpha$	α	2
$\mathbf{2}+\mathbf{2}\,\boldsymbol{\alpha}$	0	$1+2\,\alpha$	$2+\alpha$	$2+2\,\alpha$	α	1	$1+\alpha$	2	$2\,\alpha$

En fait, ces trois extensions sont encore $\mathbb{Z}/3\mathbb{Z}$-isomorphes ! Il y a des isomorphismes :

$$\begin{aligned}\varphi\colon\mathbb{K}\to\mathbb{L},&\qquad \alpha\mapsto\varphi(\alpha)=\beta-1\,;\\ \psi\colon\mathbb{K}\to\mathbb{M},&\qquad \alpha\mapsto\psi(\alpha)=\gamma+1.\end{aligned}$$

On vérifie en effet que $(\beta-1)^2=(\gamma+1)^2=2$. À isomorphisme près, il n'y a donc qu'une seule extension quadratique de $\mathbb{Z}/3\mathbb{Z}$. Elles se réalisent néanmoins sous trois « formes » différentes.

Ceci est un fait général : comme on le verra dans le chapitre suivant, pour tout p premier et tout n, il n'existe qu'une unique extension de $\mathbb{Z}/p\mathbb{Z}$ de degré n, à isomorphisme près.

Section III.D. Polynômes cyclotomiques

Terminons ce chapitre par une classe importante de polynômes, les polynômes cyclotomiques.

§ III.D(a) Racines de l'unité

Définition III.D.1. Soit $\mathbb{K}$ un corps. On dit que $\zeta \in \mathbb{K}$ est une *racine de l'unité* s'il existe un entier $n \geq 1$ tel que $\zeta^n = 1$. On note l'ensemble des racines $n$ièmes de l'unité par :

$$\mu_n(\mathbb{K}) \coloneqq \{\, \zeta \in \mathbb{K} \mid \zeta^n = 1 \,\}.$$

Remarque III.D.2. Si n divise m, alors $\mu_m(\mathbb{K}) \subset \mu_n(\mathbb{K})$.

Exemple III.D.3. On a $\mu_n(\mathbb{Q}) = \mu_n(\mathbb{R}) = \{1\}$ si n est impair et $\mu_n(\mathbb{Q}) = \mu_n(\mathbb{R}) = \{\pm 1\}$ si n est pair. Dans $\mathbb{C}$, on a :

$$\mu_n(\mathbb{C}) = \left\{ \exp(2ik\pi/n) \;\middle|\; k \in \{0, \dots, n-1\} \right\}.$$

Proposition III.D.4. Si $\mathbb{K}$ est un corps et $n \geq 1$ est un entier, alors $\mu_n(\mathbb{K})$ est un groupe cyclique de cardinal inférieur ou égal à n.

Démonstration. Il est clair que $\mu_n(\mathbb{K})$ est un sous-groupe de $\mathbb{K}^\times$. Comme $\mathbb{K}$ est un corps, le polynôme $X^n - 1$ admet au plus n racines, donc $|\mu_n(\mathbb{K})| \leq n$. On peut adapter sans difficultés la preuve du **Lemme I.D.9** pour démontrer qu'un sous-groupe fini de $\mathbb{K}^\times$ est toujours cyclique, même si $\mathbb{K}$ n'est pas lui-même fini. ◇

Remarque III.D. La dérivée de $P_n = X^n - 1$ est $P_n' = nX^{n-1}$. Si $\mathrm{car}(\mathbb{K})$ ne divise pas n, alors la seule racine de P_n' est 0 qui n'est pas une racine de P_n, donc toutes les racines de P_n sont simples. Si au contraire $\mathrm{car}(\mathbb{K}) = p$ divise n, alors toutes les racines de P_n sont multiplies (car alors $P_n' = 0$). On peut en fait vérifier que $X^{pk} - 1 = (X^k - 1)^p$ si $n = pk$, donc $\mu_{pk}(\mathbb{K}) = \mu_k(\mathbb{K})$.

Hypothèse III.D.5. Quitte à factoriser toutes les puissances de p, on supposera donc dans la suite que si $\mathrm{car}(\mathbb{K}) = p$ n'est pas nulle, alors n et p sont premiers entre eux.

On notera dans cette section $\mathbb{K}_n$ le corps de décomposition de $X^n - 1 \in \mathbb{K}[X]$. Le polynôme $X^n - 1$ y est scindé et admet donc n racines, deux à deux distinctes grâce à l'hypothèse précédente. On a donc $\mu_n(\mathbb{K}_n) \cong \mathbb{Z}/n\mathbb{Z}$. Comme $\mu_n(\mathbb{K})$ est un sous-groupe de $\mu_n(\mathbb{K}_n)$, son ordre est un diviseur de n.

Définition III.D.6. Une racine $n$ième primitive de $1 \in \mathbb{K}$ est un générateur de $\mu_n(\mathbb{K}_n)$, c'est-à-dire un élément $\zeta \in \mathbb{K}_n$ tel que $\zeta^n = 1$ et $\zeta^d \neq 1$ pour $d < n$. On note l'ensemble des racines primitives :

$$\mu_n^*(\mathbb{K}) \coloneqq \{\, \zeta \in \mu_n(\mathbb{K}_n) \mid \zeta \text{ engendre } \mu_n(\mathbb{K}_n) \,\}.$$

Attention à la notation : contrairement à $\mu_n(\mathbb{K})$, en général $\mu_n^*(\mathbb{K})$ n'est pas inclus dans $\mathbb{K}$.

Proposition III.D.7. Le cardinal de $\mu_n^*(\mathbb{K})$ est $\varphi(n)$ (l'indicatrice d'Euler).

Démonstration. Si ζ est une racine primitive $n$ième de l'unité, alors les autres racines primitives $n$ièmes sont les ζ^k avec $k \wedge n = 1$. De plus, si $k, l \in \{0, \dots, n-1\}$ sont tels que $\zeta^k = \zeta^l$, alors $\zeta^{k-l} = 1$. Comme ζ est une racine primitive, cela entraîne que $k - l = 0$. Donc $\mu_n^*(\mathbb{K})$ contient autant d'éléments qu'il y a d'entiers $0 \leq k \leq n$ premiers avec n, c'est-à-dire $\varphi(n)$. ◇

Remarque III.D.8. Si $\Bbbk \subset \mathbb{K}$ est le sous-corps premier ($\Bbbk = \mathbb{Q}$ ou $\Bbbk = \mathbb{Z}/p\mathbb{Z}$ suivant la caractéristique), alors le corps de décomposition de $X^n - 1 \in \mathbb{K}[X]$ est une extension du corps de

décomposition de $X^n - 1 \in \Bbbk[X]$, et toutes ses racines sont dans ce sous-corps de décomposition. On pourra donc supposer que $\mathbb{K} = \Bbbk$ dans la suite, et ne considérer que $\mathbb{Q}$ ou $\mathbb{Z}/p\mathbb{Z}$.

Remarque III.D.9. Si p (premier) divise $n = pk$, alors il n'y a pas de racine primitive $n$ième de l'unité dans un corps de caractéristique p d'après la **Remarque III.D** : si $x^n = x^{pk} = 1$ alors $x^k = 1$.

Exemple III.D.10. Les racines primitives $n$ièmes de $1 \in \mathbb{Q}$ sont :

$$\mu_n^*(\mathbb{Q}) \coloneqq \{\exp(2ik\pi/n) \mid k \in \{1, \dots, n-1\},\ k \wedge n = 1\}.$$

§ III.D(b) Définition et premières propriétés

Comme avant, on fixe un corps $\mathbb{K}$ (soit $\mathbb{Q}$, soit $\mathbb{Z}/p\mathbb{Z}$), un entier $n \geq 1$, et $\mathbb{K}_n$ le corps de décomposition de $X^n - 1 \in \mathbb{K}[X]$. Enfin si $car(\mathbb{K}) = p > 0$ on suppose que $n \wedge p = 1$.

Définition III.D.11. Le $n$ième *polynôme cyclotomique* $\Phi_{n,\mathbb{K}} \in \mathbb{K}_n[X]$ est le polynôme :

$$\Phi_{n,\mathbb{K}} \coloneqq \prod_{\zeta \in \mu_n^*(\mathbb{K})} (X - \zeta).$$

En d'autres termes, $\Phi_{n,\mathbb{K}}$ est l'unique polynôme qui est : unitaire ; scindé ; à racines simples ; ses racines sont les racines primitives $n$ièmes de l'unité. Dans la suite, on omettra l'indice $\mathbb{K}$, sauf si cela a une importance. D'après ce qui précède,

$$\deg\left(\Phi_{n,\mathbb{K}}\right) = \varphi(n).$$

Proposition III.D.12. Étant donné $n \geq 1$, on a :

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

Démonstration. On a l'égalité suivante, qui donne directement le résultat en notant que tous les polynômes qui interviennent sont scindés à racines simples dans $\mathbb{K}_n$:

$$\{x \in \mathbb{K}^n \mid x^n = 1\} = \mu_n(\mathbb{K}_n) = \bigcup_{d|n} \mu_d^*(\mathbb{K}) = \bigcup_{d|n} \{x \in \mathbb{K}_n \mid \Phi_d(x) = 0\}. \qquad \diamond$$

Cette formule permet de calculer Φ_n par récurrence.

1. On a bien sûr $\Phi_1 = X - 1$: la seul racine « unième » de l'unité est 1 lui-même.
2. Comme $\Phi_1\Phi_2 = X^2 - 1 = (X-1)(X+1)$, on a $\Phi_2 = X + 1$.
3. De la même manière, $\Phi_1\Phi_3 = X^3 - 1 = (X-1)(X^2 + X + 1)$ donc $\Phi_3 = X^2 + X + 1$.
4. On a encore $\Phi_1\Phi_2\Phi_4 = X^4 - 1 = (X^2-1)(X^2+1) = (X-1)(X+1)(X^2+1)$, donc on obtient $\Phi_4 = X^2 + 1$.
5. En continuant ainsi, on trouve $\Phi_5 = X^4 + X^3 + X^2 + X + 1$, $\Phi_6 = X^2 - X + 1$, $\Phi_8 = X^4 + 1$, $\Phi_9 = X^6 + X^3 + 1$, etc.

Exercice III.D.13. Ce calcul par récurrence peut se résumer facilement par la formule d'inversion de Möbius. Notons $\mu\colon \mathbb{N} \to \mathbb{C}$ la fonction de Möbius, définie par $\mu(n) = \sum_{\zeta \in \mu_n^*(\mathbb{C})} \zeta$ (la somme des racines primitives $n$ièmes de l'unité).

1. Démontrer que si $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ est décomposé en facteurs premiers, alors $\mu(n)$ est donné par :
   a. Si l'un des α_i est ≥ 2 alors $\mu(n) = 0$.

   b. Si tous les α_i valent 1 et r est pair, alors $\mu(n) = 1$.
   c. Si tous les α_i valent 1 et r est impair, alors $\mu(n) = -1$.
2. En déduire que μ est multiplicative : si $a \wedge b = 1$ alors $\mu(ab) = \mu(a)\,\mu(b)$.
3. Démontrer que $\sum_{d|n} \mu(n) = 0$ si $n > 1$ et que $\sum_{d|1} \mu(1) = 1$.
4. Démontrer la formule d'inversion de Möbius : si $f, g \colon \mathbb{N} \to A$ sont à valeurs dans un groupe abélien $(A, +)$, alors on a :
$$\forall n, g(n) = \sum_{d|n} f(d) \quad \Longrightarrow \quad \forall n, f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right).$$
5. En appliquant la formule au groupe abélien $(\mathbb{K}(X) \setminus \{0\},\ \times)$, en déduire que :
$$\Phi_n = \prod_{d|n} \left(X^{n/d} - 1\right)^{\mu(d)}.$$

Remarque III.D.14. La formule d'inversion de Möbius fournit la relation suivante sur l'indicatrice d'Euler :

$$\frac{\varphi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d}.$$

Exemple III.D.15. On retrouve essentiellement le calcul par récurrence précédent si l'on applique cette formule. Par exemple, pour calculer Φ_4 (dont les diviseurs positifs sont $\{1, 2, 4\}$) on trouve :

$$\begin{aligned}
\Phi_4 &= \prod_{d|4} (X^d - 1)^{\mu\left(\frac{4}{d}\right)} \\
&= \left(X^{4/4} - 1\right)^{\mu(4)} \cdot \left(X^{4/2} - 1\right)^{\mu(2)} \cdot \left(X^{4/1} - 1\right)^{\mu(1)} \\
&= (X-1)^0 \cdot (X^2 - 1)^{-1} \cdot (X^4 - 1)^1 \\
&= (X^4 - 1)/(X^2 - 1) \\
&= X^2 + 1.
\end{aligned}$$

Exercice III.D.16. Démontrer que $\Phi_{12} = X^4 - X^2 + 1$.

Il est facile de calculer Φ_q pour un nombre premier q :

Proposition III.D.17. Si q est premier, alors $\Phi_q = \sum_{k=0}^{q-1} X^k$.

Démonstration. Cela découle directement de l'équation suivante :

$$\Phi_1 \Phi_q = X^q - 1 = (X-1)(X^{q-1} + X^{q-2} + \cdots + X + 1). \qquad \diamond$$

Tous les polynômes cyclotomiques que nous avons calculé jusqu'à présent sont à coefficients entiers. Ceci n'est pas un hasard :

Proposition III.D.18. Le polynôme $\Phi_{n,\mathbb{Q}}$ est à coefficients entiers. Si $\mathbb{K}$ est un corps quelconque, alors $\Phi_{n,\mathbb{K}}$ est l'image de $\Phi_{n,\mathbb{Q}} \in \mathbb{Z}[X]$ par le morphisme canonique $\mathbb{Z} \to \mathbb{K}$.

Démonstration. Commençons par démontrer que $\Phi_n = \Phi_{n,\mathbb{Q}}$ est à coefficients entiers par récurrence. Pour $n = 1$, c'est vrai, car $\Phi_1 = X - 1$. Supposons maintenant que Φ_d est à coefficients entiers pour tout $d < n$. On pose $A = \prod_{d|n, d \neq n} \Phi_d$ qui est donc à coefficients entiers et unitaire. On peut former la division euclidienne de $X^n - 1$ par A dans l'anneau euclidien $\mathbb{Z}[X]$ pour trouver :

$$X^n - 1 = AQ + R, \qquad Q, R \in \mathbb{Z}[X], \qquad \deg(R) < \deg(A).$$

Or, dans $\mathbb{Q}[X]$, on a l'égalité $X^n - 1 = A\Phi_n$ et donc $A(\Phi_n - Q) = R$. Pour une question de degré, on doit donc avoir $\Phi_n = Q$.

Démontrons maintenant que $\Phi_{n,\mathbb{K}}$ est l'image de $\Phi_{n,\mathbb{Q}}$ sous l'application canonique $\psi\colon \mathbb{Z} \to \mathbb{K}$ pour tout corps $\mathbb{K}$. Le cas $n = 1$ est évident ($\Phi_1 = X - 1$ quel que soit le corps). On a l'égalité suivante dans $\mathbb{Z}[X]$:

$$X^n - 1 = \prod_{d|n} \Phi_{d,\mathbb{Q}} = \Phi_{n,\mathbb{Q}} \cdot \prod_{d|n, d\neq n} \Phi_{d,\mathbb{Q}}. \qquad (*)$$

L'image de $X^n - 1$ par ψ est encore $X^n - 1$, et on a l'égalité suivante dans $\mathbb{K}[X]$:

$$X^n - 1 = \prod_{d|n} \Phi_{d,\mathbb{K}} = \Phi_{n,\mathbb{K}} \cdot \prod_{d|n, d\neq n} \Phi_{d,\mathbb{K}}. \qquad (**)$$

Mais si on applique ψ à l'équation $(*)$, on trouve que $X^n - 1 = \psi\big(\Phi_{n,\mathbb{Q}}\big) \cdot \prod_{d|n,d\neq n} \Phi_{d,\mathbb{K}}$. Comme l'anneau $\mathbb{K}[X]$ est intègre, c'est que $\psi\big(\Phi_{n,\mathbb{Q}}\big) = \Phi_{n,\mathbb{K}}$. ◇

Cette proposition justifie le fait que l'on ne note plus le corps en indice de Φ_n : ils sont tous obtenus par réduction de $\Phi_{n,\mathbb{Q}} \in \mathbb{Z}[X]$.

§ III.D(c) Irréductibilité sur $\mathbb{Z}$

Théorème III.D.19. Pour tout $n \geq 1$, le polynôme cyclotomique $\Phi_n \in \mathbb{Z}[X]$ est irréductible sur $\mathbb{Z}$.

On étudiera la réductibilité de Φ_n mod p dans la Section IV.C.

Corollaire III.D.20. Si $\zeta \in \mathbb{C}$ est une racine primitive $n$ième de l'unité, alors son polynôme minimal est Φ_n et on a $[\mathbb{Q}(\zeta)\colon \mathbb{Q}] = \varphi(n)$.

Comme $c(\Phi_n)$ vaut 1, il suffit de démontrer que Φ_n est irréductible sur $\mathbb{Q}$. On rappelle que $\mathbb{Q}_n$ désigne le corps de décomposition de Φ_n sur $\mathbb{Q}$. On note aussi $\zeta \in \mathbb{Q}_n$ une racine primitive $n$ième de l'unité.

Lemme III.D.21. Le polynôme minimal F_ζ de ζ sur $\mathbb{Q}$ est à coefficients entiers.

Démonstration. L'anneau $\mathbb{Z}[X]$ est factoriel, donc on peut factoriser $\Phi_n = \pm P_1 \dots P_r$ avec $P_i \in \mathbb{Z}[X]$, uniques à permutation et signe près. Comme Φ_n est unitaire, tous les P_i le sont aussi au signe près ; quitte à factoriser par -1, on peut supposer que tous les P_i sont unitaires. Or, ζ est racine de Φ_n, donc de l'un des P_i et donc F_ζ divise ce P_i. Ce polynôme P_i est unitaire (donc de contenu 1) et irréductible sur $\mathbb{Z}$, donc il est irréductible sur $\mathbb{Q}$. On en déduit donc que $F_\zeta = P_i$ est à coefficients entiers. ◇

Lemme III.D.22. Soit p un nombre premier qui ne divise pas n. Le polynôme minimal F_{ζ^p} de ζ^p est le même que le polynôme minimal F_ζ de ζ.

Démonstration. Notons $F = F_\zeta$ et $G = F_{\zeta^p}$ pour simplifier la notation. Comme $p \wedge n = 1$, ζ^p est aussi une racine primitive $p$ième de l'unité, donc g divise aussi Φ_n. Supposons que $F \neq G$. Comme ils sont irréductibles et premiers entre eux dans $\mathbb{Z}[X]$, et qu'ils divisent tous deux Φ_n, leur produit FG divise Φ_n.

Or, $G(\zeta^p) = 0$, c'est-à-dire ζ est racine du polynôme $G(X^p)$ qui est donc divisible par F (en principe dans $\mathbb{Q}[X]$, mais comme les polynômes sont unitaire une application du lemme de Gauss donne que cela se passe en fait dans $\mathbb{Z}[X]$). On a donc $G(X^p) = FH$ avec $H \in \mathbb{Z}[X]$.

On peut réduire cette équation mod p, ce qui donne $\bar{G}(X^p) = \bar{F}\bar{H}$ (où $\bar{\cdot}$ est la réduction mod p). Mais, modulo p, on a les équations $(Q+R)^p = Q^p + R^p$ pour des polynômes Q, R et $a^p \equiv a \bmod p$ pour un entier a, donc $\bar{G}(X^p) = \left(\bar{G}(X)\right)^p$, d'où $\bar{F}\bar{H} = \bar{G}^p$. Si Q est un facteur irréductible de $\bar{F}$, alors c'est aussi un facteur irréductible de $\bar{G}^p$, donc également de $\bar{G}$ par le lemme d'Euclide. Donc le carré Q^2 divise $\bar{F}\bar{G} = \bar{\Phi}_n$. Le polynôme $\bar{\Phi}_n$ admet donc une racine double dans son corps de décomposition sur $\mathbb{Z}/p\mathbb{Z}$.C'est absurde : toutes ses racines sont simples par définition. ◇

Démonstration du théorème. D'après le lemme précédent, si p est un nombre premier qui ne divise pas n, alors ζ^p est racine de F_ζ. Si on prend maintenant $k = p_1^{\alpha_1} \dots p_r^{\alpha_r} < n$ premier avec n, une récurrence immédiate donne que le polynôme minimal de ζ^k est le même que celui de ζ. Donc finalement, tous les ζ^k avec $k \wedge n = 1$ sont des racines de F_ζ. Ces racines sont au nombre de $\varphi(n)$, donc $\deg(F_\zeta) \geq \varphi(n)$. Or F_ζ divise Φ_n qui est de degré $\varphi(n)$, donc $F_\zeta = \Phi_n$ est bien irréductible (c'est le polynôme minimal de ζ). ◇

Corollaire III.D.23. Si $\alpha \in \mathbb{C}$ est une racine primitive $m$ième de l'unité et β une racine primitive $n$ième de l'unité avec $n \wedge m = 1$, alors $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}$.

Exercice III.D.24. Si $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ avec p_i premiers deux à deux distincts, démontrer que :

$$\Phi_n = \Phi_{p_1 \dots p_r}\left(X^{p_1^{\alpha_1 - 1} \dots p_r^{\alpha_r - 1}}\right).$$

§ III.D(d) Extensions cyclotomiques

Soit p un nombre premier fixé et ζ une racine primitive $p$ième de l'unité. Rappelons un résultat vu dans la preuve de la réciprocité quadratique (§ I.E(b)). Si on note la somme quadratique de Gauss $g = \sum_{n=0}^{p-1} \zeta_p^{n^2}$, alors $g^2 = p^* = \left(\frac{-1}{p}\right) p$. On peut faire le lien entre cette équation et ce qui précède :

Définition III.D.25. Une extension $\mathbb{K} \subset \mathbb{L}$ est *quadratique* si c'est le corps de décomposition d'un polynôme irréductible de degré 2.

Définition III.D.26. Une *extension* $\mathbb{K} \subset \mathbb{L}$ est dite *cyclotomique* si elle est contenue dans le corps de décomposition de $\Phi_{n,\mathbb{K}}$; en d'autres termes, si elle est contenue dans une extension obtenue en adjoignant une racine primitive $n$ième de l'unité à $\mathbb{K}$.

Proposition III.D.27. Toute extension quadratique de $\mathbb{Q}$ est cyclotomique.

Démonstration. Une extension quadratique est de la forme $\mathbb{Q}(\sqrt{n})$ avec n entier. Si on écrit $n = (-1)^\varepsilon p_1^{2\alpha_1+1} \dots p_r^{2\alpha_r+1} p_{r+1}^{2\beta_{r+1}} \dots p_{r+s}^{2\beta_{r+s}}$ sa décomposition en nombres premiers distincts, alors $\mathbb{Q}(\sqrt{n}) = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_r})$ si $\varepsilon = 0$ et $\mathbb{Q}(\sqrt{n}) = \mathbb{Q}(i, \sqrt{p_1}, \dots, \sqrt{p_r})$ sinon.

Par récurrence, il suffit donc de démontrer que $\mathbb{Q}(i)$ et chaque $\mathbb{Q}(\sqrt{p})$ est cyclotomique. En effet, si on a une racine primitive $m$ième ζ_m et une racine primitive $n$ième ζ_n, alors $\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{m \vee n})$. En d'autres termes, une extension cyclotomique d'une extension cyclotomique est cyclotomique.

On a bien sûr $\mathbb{Q}(i) = \mathbb{Q}(\zeta_4)$ qui est cyclotomique. Grâce à la formule sur la somme quadratique de Gauss, $\mathbb{Q}(\sqrt{p})$ est contenue soit dans $\mathbb{Q}(\zeta_p)$ (si $\left(\frac{-1}{p}\right) = 1$) soit dans $\mathbb{Q}(\zeta_4, \zeta_p)$ (si $\left(\frac{-1}{p}\right) = -1$), ce qui permet de conclure. ◇

Remarque III.D.28. Les extensions quadratiques sont des cas particuliers d'extensions abéliennes (voir le Chapitre V). Un théorème de Kronecker dit que toute extension abélienne est cyclotomique, mais la preuve est bien plus ardue.

Chapitre IV. Corps finis

« Le temps du monde fini commence. »

Paul Valéry, *Regards sur le monde actuel*

Section IV.A. Morphisme de Frobenius

Nous avons déjà remarqué que, dans le corps $\mathbb{Z}/p\mathbb{Z}$, la « formule magique » suivante est vraie :

$$\forall a, b \in \mathbb{Z}/p\mathbb{Z}, \qquad (a+b)^p = a^p + b^p.$$

Cette observation se généralise amplement.

Proposition IV.A.1. Soit $\mathbb{K}$ un corps de caractéristique $p > 0$. L'application $F : \mathbb{K} \to \mathbb{K}$ définie par $F(x) := x^p$ est un morphisme de corps. Si $\mathbb{K}$ est fini, c'est un automorphisme ; si $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$, c'est l'identité.

Démonstration. Il est clair que F vérifie $F(1) = 1$ et $F(xy) = F(x)\,F(y)$. De plus, pour tous $x, y \in \mathbb{K}$, on a :

$$F(x+y) = (x+y)^p = x^p + \binom{p}{1} x^{p-1}y + \cdots + \binom{p}{p-1} xy^{p-1} + y^p.$$

Or, p divise $\binom{p}{k}$ pour tout $k \in \{1, \dots, p-1\}$, donc on a bien $F(x+y) = F(x) + F(y)$.

Un morphisme de corps est toujours injectif. Si $\mathbb{K}$ est fini, alors $F : \mathbb{K} \to \mathbb{K}$ est donc également surjectif et c'est donc un automorphisme. Enfin, si $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$, alors le théorème de Fermat dit bien que $F(x) = x^p = x \pmod p$. ◇

Définition IV.A.2. Soit $\mathbb{K}$ un corps de caractéristique p. Le morphisme de la proposition précédente s'appelle le *morphisme de Frobenius* (ou automorphisme de Frobenius si $\mathbb{K}$ est fini) et se note $\mathrm{Frob}_{\mathbb{K}} : \mathbb{K} \to \mathbb{K}$.

Remarque IV.A.3. Si $\mathbb{K}$ n'est pas fini, en général $\mathrm{Frob}_{\mathbb{K}}$ n'est pas un isomorphisme. Par exemple, si $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}(X)$, alors il n'existe pas de fraction rationnelle $F(X) = P(X)/Q(X)$ telle que $\mathrm{Frob}\big(F(X)\big) = F(X)^p = X$.

Proposition IV.A.4. Soit $\mathbb{K}$ un corps de caractéristique $p > 0$. L'ensemble des points fixes de $\mathrm{Frob}_{\mathbb{K}}$ est le sous-corps premier de $\mathbb{K}$.

Démonstration. Les points fixes de $\mathrm{Frob}_{\mathbb{K}}$ sont les racines de $X^p - X$. Les p éléments du sous-corps premier $\mathbb{Z}/p\mathbb{Z} \subset \mathbb{K}$ vérifient l'équation $x^p = x$ d'après le petit théorème de Fermat. Comme $\mathbb{K}$ est un corps, le polynôme $X^p - X$ ne peut avoir au plus que $\deg(X^p - X) = p$ racines dans $\mathbb{K}$, donc ce sont exactement les éléments du sous-corps premier. ◇

Section IV.B. Existence et unicité de $\mathbb{F}_q$

Tous les corps finis ont un cardinal de la forme $q = p^n$ avec p premier et $n \geq 1$. On connaît un corps de cardinal p : le corps $\mathbb{Z}/p\mathbb{Z}$. On a de plus vu dans le § III.C(c) quelques exemples de corps finis à l'aide d'extensions algébriques de $\mathbb{Z}/p\mathbb{Z}$, de cardinaux $2^2 = 4$, $2^3 = 8$, et $3^2 = 9$. On a de plus remarqué que pour un cardinal donné, les extensions trouvées sont isomorphes entre elles. On est en droit de se demander s'il s'agit d'un fait général ; la réponse est oui !

Proposition IV.B.1. Soit p un nombre premier et $n \geq 1$ un entier. Il existe un corps de cardinal $q = p^n$ qui est unique à isomorphisme près. Ce corps est le corps de décomposition de $X^q - X \in \mathbb{Z}/p\mathbb{Z}[X]$.

Démonstration. Démontrons d'abord qu'un corps à $q = p^n$ éléments existe. Soit $\mathbb{L}$ le corps de décomposition de $P = X^q - X$ sur $\mathbb{Z}/p\mathbb{Z}$. L'ensemble des racines de P forme un sous-corps $\mathbb{L}' \subset \mathbb{L}$ (en appliquant la « formule magique » plusieurs fois). Par minimalité du corps de décomposition, on a donc $\mathbb{L}' = \mathbb{L}$. Le polynôme P admet $\deg(P) = q$ racines, potentiellement multiples. Mais la dérivée de P vaut $P' = qX^{q-1} - 1 = -1$ (car $p|q$) qui n'admet aucune racine, donc les racines de P sont toutes simples. On a donc $|\mathbb{L}| = q = p^n$.

Supposons maintenant que $\mathbb{M}$ est un autre corps à $q = p^n$ éléments. Le groupe des unités $\mathbb{M}^\times$ est de cardinal $q - 1$, donc tous ses éléments vérifient $x^{q-1} = 1$. Tous les éléments de $\mathbb{M}$ vérifient donc $x^q = x$ et les q éléments de $\mathbb{M}$ sont donc les racines de $X^q - X$. Le corps $\mathbb{M}$ est donc un corps de décomposition de $X^q - X$ sur $\mathbb{Z}/p\mathbb{Z}$ et donc isomorphe au corps $\mathbb{L}$ trouvé ci-dessus. ◇

Définition IV.B.2. Soit $q = p^n$ une puissance du nombre premier p. On notera $\mathbb{F}_q$ l'unique corps de cardinal q.

Exemple IV.B.3. Pour $q = p = p^1$, on $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. On a décrit $\mathbb{F}_4$, $\mathbb{F}_8$ et $\mathbb{F}_9$ dans le § III.C(c).

Section IV.C. Polynômes à coefficients dans $\mathbb{F}_q$

Nous avons vu dans la Section II.E divers critères qui permettent de déterminer quand un polynôme à coefficients dans un anneau factoriel A est irréductible. La plupart de ces critères sont principalement utiles quand $A = \mathbb{Z}$. Ici, nous allons voir deux autres critères utiles pour les corps finis (mais qui peuvent également s'appliquer à $\mathbb{Q}$).

Théorème IV.C.1. Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$ un polynôme de degré $n > 0$. Le polynôme P est irréductible sur $\mathbb{K}$ si et seulement s'il n'a pas de racines dans les extensions $\mathbb{K} \subset \mathbb{L}$ de degré $[\mathbb{L}:\mathbb{K}] \leq n/2$.

Démonstration. Il y a deux cas possibles :

- Si P est irréductible sur $\mathbb{K}$, et si $\alpha \in \mathbb{L}$ est une racine de P, alors P est le polynôme minimal de α sur $\mathbb{K}$ et $[\mathbb{K}(\alpha):\mathbb{K}] = n$ et donc $[\mathbb{L}:\mathbb{K}] \geq [\mathbb{K}(\alpha):\mathbb{K}] = n$.
- Si au contraire P est réductible, alors on a $P = QR$ avec $\deg(Q), \deg(R) > 0$. L'un des deux est de degré $\leq n/2$, disons $\deg(Q) \leq n/2$. Pour Q' un facteur irréductible de Q et $\mathbb{L}$ son corps de rupture, on a $[\mathbb{L}:\mathbb{K}] = \deg(Q') \leq \deg(Q) \leq n/2$, et P admet une racine dans $\mathbb{L}$. ◇

Exemple IV.C.2. Le polynôme $X^4 - X + 1$ est irréductible sur $\mathbb{F}_2$. En effet, il suffit de vérifier qu'il n'a pas de racine dans $\mathbb{F}_4$ (par un calcul immédiat). On en déduit que ce polynôme est irréductible sur $\mathbb{Z}$ en appliquant le **Théorème II.E.18**.

Exercice IV.C.3. Démontrer que $X^{p^2} - X + 1$ est irréductible sur $\mathbb{Z}$ quel que soit p premier.

Exemple IV.C.4. On peut se servir de ce résultat pour démontrer à nouveau que le polynôme $\Phi_8 = X^4 + 1$ est réductible sur $\mathbb{F}_p$ pour tout $p > 2$ (le cas $p = 2$ étant évident). Il suffit en effet de vérifier que Φ_8 a une racine dans $\mathbb{F}_{p^2}$, la seule extension de degré 2 de $\mathbb{F}_p$. Or une racine de Φ_8 dans un corps $\mathbb{K}$ n'est rien d'autre qu'une racine primitive huitième de l'unité, c'est-à-dire un élément $x \in \mathbb{K}^\times$ d'ordre 8. On a démontré précédemment que, $\mathbb{F}_{p^2}^\times = \mathbb{Z}/(p^2 - 1)\mathbb{Z}$. Il suffit donc de démontrer que 8 divise

p^2-1 (car alors $\mathbb{F}_{p^2}^\times$ contiendra un élément d'ordre 8). On a $p^2-1=(p-1)(p+1)$, chacun de ces deux termes est pair, et l'un des deux est multiple de 4, donc le produit est bien divisible par 8. ◇

Remarque IV.C.5. On peut également se servir de la réciprocité quadratique pour démontrer le résultat :

- Si $p \equiv 1 \mod 4$, alors d'après le premier complément de la réciprocité quadratique, -1 est un résidu quadratique, disons $-1 \equiv a^2 \mod p$ et alors
$$\Phi_8 \equiv (X^2-a)(X^2+a) \mod p$$
- Si au contraire $p \equiv 3 \mod 4$, il y a encore plusieurs cas :
  - Si $p \equiv 7 \mod 8$, alors $2 \equiv b^2 \mod p$ est un résidu quadratique d'après le second complément de la réciprocité quadratique, et on a une décomposition :
$$\Phi_8 \equiv (X^2+aX+1)(X^2-aX+1) \mod p.$$
  - Enfin, si $p \equiv 3 \pmod 8$, alors ni -1 ni 2 ne sont des résidus quadratiques, donc $-2 \equiv c^2 \mod p$ est un résidu quadratique. On a alors la décomposition :
$$\Phi_8 \equiv (X^2+cX-1)(X^2-cX-1) \mod p.$$

Nous sommes en droit de nous demander s'il s'agit d'un cas isolé ou d'un fait général. La table suivante résume la situation pour les petites valeurs de n et p.

Table IV.C-a La case contient ✓ si Φ_n est irréductible mod p et rien sinon.

	Φ_1	Φ_2	Φ_3	Φ_4	Φ_5	Φ_6	Φ_7	Φ_8	Φ_9	Φ_{10}	Φ_{11}	Φ_{12}	Φ_{13}	Φ_{14}	Φ_{15}
$p=2$	✓	✓	✓		✓	✓			✓	✓	✓		✓		
$p=3$	✓	✓		✓	✓		✓			✓				✓	
$p=5$	✓	✓	✓			✓	✓		✓					✓	
$p=7$	✓	✓		✓	✓					✓	✓		✓		
$p=11$	✓	✓	✓	✓		✓			✓				✓		
$p=13$	✓	✓			✓					✓	✓				
$p=17$	✓	✓	✓		✓	✓	✓			✓	✓			✓	
$p=19$	✓	✓		✓			✓				✓		✓	✓	
$p=23$	✓	✓	✓	✓	✓	✓			✓	✓					
$p=29$	✓	✓	✓			✓			✓		✓				
$p=31$	✓	✓		✓			✓							✓	
$p=37$	✓	✓			✓					✓			✓		

Le théorème suivant donne une partie de la réponse :

Théorème IV.C.6. Soit $n \geq 1$ un entier. Il existe un nombre premier p qui ne divise pas n et tel que Φ_n est irréductible sur $\mathbb{F}_p$ si et seulement si $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique.

Remarque IV.C.7. On a vu dans la Section I.D que $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si et seulement si $n=1, 2, 4$, q^α ou $2q^\alpha$ avec q premier impair. Cela explique les colonnes vides pour $n=8, 12, 15$ (qui ne sont pas de cette forme) dans la table ci-dessus.

La preuve de ce théorème repose sur le résultat suivant, qui généralise le fait qu'il y a une infinité de nombres premiers congrus à $1 \bmod 4$, ou à $-1 \bmod 8$:

Théorème IV.C.8 (Théorème de la progression arithmétique, Dirichlet). Soit $a, n \geq 1$ deux entiers premiers entre eux. Il existe une infinité de nombres premiers congrus à $a \bmod n$.

Lemme IV.C.9. Le polynôme Φ_n est réductible sur $\mathbb{F}_p$ (où p est premier et ne divise pas n) si et seulement si $p \in (\mathbb{Z}/n\mathbb{Z})^\times$ est d'ordre $< \varphi(n)$.

Démonstration. En utilisant le **Théorème IV.C.1**, Φ_n est réductible sur $\mathbb{F}_p$ si et seulement s'il existe $m \leq \varphi(n)/2$ tel que Φ_n a une racine dans $\mathbb{F}_{p^m}$. Or les racines de Φ_n sont les racines primitives $n$ièmes de l'unité, donc cela revient à demander que $\mathbb{F}_{p^m}^\times$ contient un élément d'ordre n. Comme $\mathbb{F}_{p^m}^\times$ est cyclique d'ordre $p^m - 1$, cela revient à avoir $n | p^m - 1$, ou encore que $p^m \equiv 1 \pmod n$, ou encore que p est d'ordre $\leq m < \varphi(n)$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$ (car un sous-groupe propre est d'indice au moins 2). ◇

Démonstration du théorème. Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est d'ordre $\varphi(n)$. S'il n'est pas cyclique, tous ses éléments sont d'ordre $< \varphi(n)$, donc en particulier p est d'ordre $< \varphi(n)$. Réciproquement, si $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique, notons $\alpha \in (\mathbb{Z}/n\mathbb{Z})^\times$ un générateur. D'après le théorème de la progression arithmétique, il existe une infinité de nombres premiers dans la classe α, donc en tout cas au moins un, disons $\alpha = [p]$ avec $p \in \mathbb{Z}$ premier. Alors cet élément est d'ordre $\varphi(n)$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$ et donc Φ_n est irréductible mod p. ◇

Notons que le lemme ci-dessus admet la généralisation suivante :

Proposition IV.C.10. Soit n un entier et p un premier qui ne divise pas n et soit d l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^\times$. Sur $\mathbb{F}_p$, le polynôme cyclotomique Φ_n se décompose en un produit de $\varphi(n)/d$ facteurs irréductibles, chacun de degré d.

Démonstration. Soit $\zeta \in \overline{\mathbb{F}}_p$ une racine primitive $n$ième de l'unité et d l'ordre de p dans le groupe des inversibles mod n, de telle sorte qu'on a un plongement :

$$\mathbb{Z}/d\mathbb{Z} \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times, \qquad k \mapsto p^k.$$

Le quotient $G = (\mathbb{Z}/n\mathbb{Z})^\times/(\mathbb{Z}/d\mathbb{Z})$ est d'ordre $\varphi(n)/d$, et on note ses classes $[a]$ pour $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. On a alors l'égalité, où l'on écrit $[a] \in G$ pour exprimer le choix d'un représentant $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ par classe modulo le sous-groupe $\{1, p, p^2, \dots, p^{d-1}\}$:

$$\Phi_n = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} (X - \zeta^k) = \prod_{[a] \in G} \prod_{l=0}^{d-1} \left(X - \zeta^{p^l a}\right).$$

Chacun des polynômes $P_a := \prod_{l=0}^{d-1} \left(X - \zeta^{p^l a}\right) \in \overline{\mathbb{F}}_p$ est de degré d et ils sont au nombre de $\varphi(n)/d$. Il nous faut montrer que $P_a \in \mathbb{F}_p[X]$ et qu'il est irréductible.

Pour montrer que $P_a \in \mathbb{F}_p[X]$, nous allons montrer qu'il est invariant par l'endomorphisme de Frobenius, dont les points fixes sont justement les éléments du sous-corps premier $\mathbb{F}_p$. On a que :

$$\mathrm{Frob}_p(P_a) = \prod_{l=1}^{d-1} \left(X - \left(\zeta^{p^l a}\right)^p\right) = \prod_{l=0}^{d-1} \left(X - \zeta^{p^{l+1} a}\right).$$

Ce dernier polynôme est bien égal à P_a, car $x \mapsto px$ est une bijection sur $\{a, pa, p^2 a, \dots, p^{d-1} a\}$.

Démontrons enfin que P_a est irréductible dans $\mathbb{F}_p$. Si au contraire il était irréductible, il admettrait une racine dans l'unique extension de degré $m \leq \deg(P_a)/2 = d/2$ de $\mathbb{F}_p$, à savoir $\mathbb{F}_{p^m}$. Or une racine de P_a est une racine de Φ_n, c'est-à-dire une racine primitive $n$ième de l'unité, ou encore un élément d'ordre n dans $\mathbb{F}_{p^m}^\times$. Si une telle racine existe, par le théorème de Lagrange, $n | p^m - 1$ ou encore $p^m \equiv 1 \pmod n$. C'est absurde, car cela signifierait que d, l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^\times$, serait inférieur à $m \leq d/2 < d$. ◇

Exemple IV.C.11. Le nombre premier $p = 7$ est d'ordre 3 modulo $n = 18$ (car $7^3 \equiv 1 \pmod{18}$ mais $7^2 \not\equiv 1 \pmod{18}$). On a de plus $\varphi(n) = \varphi(2)\,\varphi(3^2) = 3(3-1) = 6$. Le polynôme Φ_{18}, de degré

$\varphi(18) = 6$, se décompose donc en un produit de $\varphi(18)/3 = 2$ polynômes, chacun de degré 3, sur $\mathbb{F}_7$. On vérifie qu'effectivement,

$$\Phi_{18} = X^6 - X^3 + 1 \equiv (X^3 + 2)(X^3 + 4) \pmod 7.$$

Le théorème suivant donne encore un autre critère d'irréductibilité :

Théorème IV.C.12. Soit $\mathbb{K}$ un corps, $P \in \mathbb{K}[X]$ un polynôme irréductible, et $\mathbb{K} \subset \mathbb{L}$ une extension. Si $d = \deg(P)$ et $m = [\mathbb{L}:\mathbb{K}]$ sont premiers entre eux, alors P est irréductible sur $\mathbb{L}$.

Démonstration. Supposons au contraire que $P = QR$ dans $\mathbb{L}[X]$ avec Q irréductible unitaire de degré $q \in \{1, \dots, d-1\}$. Soit $\mathbb{L}[X]/(Q) = \mathbb{L}(\alpha)$ un corps de rupture de Q. Alors $[\mathbb{L}(\alpha):\mathbb{L}] = q$, et $[\mathbb{K}(\alpha):\mathbb{K}] = d$ car $\mathbb{K}(\alpha)$ est un corps de rupture de P sur $\mathbb{K}$. Si on pose $r = [\mathbb{L}(\alpha):\mathbb{K}(\alpha)]$, par multiplicativité des degrés, on obtient :

$$[\mathbb{L}(\alpha):\mathbb{L}] \cdot [\mathbb{L}:\mathbb{K}] = [\mathbb{L}(\alpha):\mathbb{K}(\alpha)] \cdot [\mathbb{K}(\alpha):\mathbb{K}] \Longrightarrow qm = rd.$$

Comme $d \wedge m = 1$, on en déduit que d divise q. Or $q < d$, donc c'est absurde. ◇

Exemple IV.C.13. Supposons que P est un polynôme de degré 2 qui n'admet pas de racines sur $\mathbb{F}_p$. Il est donc irréductible, et par le théorème il est donc irréductible sur $\mathbb{F}_{p^n}$ pour tout n impair.

Section IV.D. Théorème de Weddeburn ☆

Définition IV.D.1. Un *corps gauche* est un anneau unitaire $\mathbb{D}$ (non nécessairement commutatif) tel que $1 \neq 0$ et tout élément non nul admet un inverse pour la multiplication (c'est-à-dire

$$\forall x \in \mathbb{D} \setminus \{0\}, \qquad \exists y \in \mathbb{D}, \qquad xy = yx = 1.$$

Exemple IV.D.2. Un corps est un exemple de corps gauche.

Exemple IV.D.3. Il existe des exemples de corps gauches qui ne sont pas des corps. Un exemple est donné par l'ensemble des quaternions $\mathbb{H}$. Un quaternion est un nombre de la forme $a + bi + cj + dk$, où les symboles i, j, k sont des « unités imaginaires[14] » (comme $i \in \mathbb{C}$) et $a, b, c, d \in \mathbb{R}$ sont des réels. L'addition se fait coefficient par coefficient, et la multiplication est l'unique application $\mathbb{R}$-bilinéaire telle que :

$$i^2 = j^2 = k^2 = ijk = -1.$$

On vérifiera que la multiplication est associative, unitaire, et que tout élément non nul admet un inverse. Ce corps n'est pas commutatif : par exemple, $ij = k = -ji$.

Remarque IV.D.4. On peut représenter un quaternion $a + bi + cj + dk$ comme une matrice 2×2 à coefficients complexes (l'addition et la multiplication sont celles des matrices) :

$$a + bi + cj + dk \in \mathbb{H} :: \begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix} \in \mathcal{M}_2(\mathbb{C}).$$

On obtient ainsi un isomorphisme entre $\mathbb{H}$ et un sous-anneau de $\mathcal{M}_2(\mathbb{C})$. Cette représentation fait écho à la représentation traditionnelle d'un nombre complexe $a + bi$ ($a, b \in \mathbb{R}$) sous la forme d'une matrice réelle 2×2 :

[14] Le symbole j employé ici n'a rien à voir avec la racine cubique de l'unité $j = \exp(2i\pi/3)$.

$$a + bi \in \mathbb{C} :: \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathcal{M}_2(\mathbb{R}).$$

Le théorème suivant dit que cette situation, celle d'un anneau qui vérifie tous les axiomes d'un corps mais qui n'est pas commutatif, ne peut pas se produire pour les anneaux finis :

Théorème IV.D.5 (Weddeburn). Tout corps gauche fini est commutatif.

Démonstration. Soit $\mathbb{K}$ un corps gauche fini. On note son centre $Z \subset \mathbb{K}$, l'ensemble des éléments qui commutent avec tous les autres :

$$Z = \{\, a \in \mathbb{K} \mid \forall x \in \mathbb{K},\ ax = xa \,\}.$$

Il n'est pas difficile de vérifier que Z est un sous-corps (commutatif !) de $\mathbb{K}$. Notons $q = p^n$ le cardinal de $Z \cong \mathbb{F}_q$. On vérifie sans peine que $\mathbb{K}$ est un espace vectoriel sur Z, donc pour $d = \dim_Z \mathbb{K}$, on a $|\mathbb{K}| = q^d$. L'objectif sera bien entendu de démontrer que $\mathbb{K} = Z$, c'est-à-dire que $d = 1$. Supposons au contraire que $d > 1$ dans la suite pour arriver à une contradiction.

Le groupe (non-abélien) $\mathbb{K}^\times = \mathbb{K} \setminus \{0\}$ agit sur lui-même par conjugaison, c'est-à-dire qu'on pose, pour $g \in \mathbb{K}^\times$ et $x \in \mathbb{K}^\times$:

$$g \cdot x \coloneqq gxg^{-1}.$$

Étant donné $x \in \mathbb{K}^\times$, on note son orbite et son « stabilisateur » (on rajoute l'élément nul) par :

$$\omega(x) \coloneqq \{\, gxg^{-1} \in \mathbb{K}^\times \mid g \in \mathbb{K}^\times \,\}, \qquad \mathrm{Stab}(x) \coloneqq \{\, g \in \mathbb{K}^\times \mid gx = xg \,\} \cup \{0\}.$$

Pour tout $x \in \mathbb{K}^\times$, le sous-ensemble $\mathrm{Stab}(x)$ est un sous-corps de $\mathbb{K}$ (non nécessairement commutatif), et le (vrai) stabilisateur de x sous l'action est $\mathrm{Stab}(x)^\times$. Comme ci-dessus, pour $d_x = \dim_Z \mathrm{Stab}(x) \leq d$, on a $|\mathrm{Stab}(x)| = q^d$. On obtient donc, d'après le rapport habituel entre cardinal de l'orbite et cardinal du stabilisateur :

$$|\omega(x)| = \frac{q^d - 1}{q^{d_x} - 1}.$$

De plus, le groupe $\mathrm{Stab}(x)^\times$ est un sous-groupe de $\mathbb{K}^\times$, donc leurs ordres se divisent l'un l'autre, c'est-à-dire $q^{d_x} - 1 | q^d - 1$. Comme $q \geq 2$, cela entraîne $d_x | d$. En passant aux polynômes cyclotomiques, on obtient :

$$|\omega(x)| = \frac{q^d - 1}{q^{d_x} - 1} = \frac{\prod_{k|d} \Phi_k(q)}{\prod_{k|d_x} \Phi_k(q)} = \prod_{k|d,\ \neg(k|d_x)} \Phi_k(q).$$

Si $d_x = d$, alors bien sûr $|\omega(x)| = 1$. Mais si au contraire $d_x < d$, c'est-à-dire $x \notin Z$, alors $\Phi_d(q)$ divise le nombre entier $\frac{q^d - 1}{q^{d_x} - 1}$.

D'après l'équation des classes, on a :

$$|\mathbb{K}^\times| = |Z^\times| + \sum_{x \notin Z} |\omega(x)|.$$

Cela entraîne donc :

$$q^d - 1 = q - 1 + \sum_{x \notin Z} \frac{q^d - 1}{q^{d_x} - 1}.$$

Comme $\Phi_d(q)$ divise $q^d - 1$ et la somme, il divise aussi $q - 1$, et en particulier :

$$|\Phi_d(q)| \leq q - 1.$$

On sait par ailleurs que $\Phi_d(q) = (q - \zeta_1) \dots (q - \zeta_{\varphi(d)})$ où les ζ_i sont les racines primitives $d$ièmes de l'unité. Comme $d > 1$, aucune de ces racines (qui sont de module 1) ne vaut 1, donc pour tout i, $|q - \zeta_i| > q - 1$ (faire un dessin). Cela entraîne donc que :

$$|\Phi_d(q)| > (q-1)^{\varphi(d)} \geq q - 1.$$

Cela contredit l'inégalité précédente. ◇

Remarque IV.D.6. Il existe des corps gauches de caractéristique non nulle, mais leur construction dépasse le cadre de ce que l'on a appris jusqu'ici.

Section IV.E. Théorie de Galois des corps finis

La théorie de Galois consiste en l'étude des extensions de corps et de leurs automorphismes via une correspondance avec un certain groupe de transformations. Avant d'étudier la théorie de Galois en toute généralité dans le Chapitre V, nous allons commencer par l'étudier dans un cas très simple, celui des corps finis. On récapitule ce qui a été vu dans les sections précédentes :

- Tout corps fini a pour cardinal une puissance d'un nombre premier, $q = p^n$.
- Pour chaque $q = p^n$, il existe un corps $\mathbb{F}_q$ de cardinal q, unique à isomorphisme près.
- Le corps $\mathbb{F}_q$ est le corps de décomposition de $X^q - X \in \mathbb{F}_p[X]$. En particulier, pour tout $x \in \mathbb{F}_q$, on a $x^q = x$.
- L'application $\mathrm{Frob}_p : \mathbb{F}_q \to \mathbb{F}_q$, $x \mapsto x^p$ est un automorphisme de corps. L'ensemble de ses points fixes est le sous-corps premier $\mathbb{F}_p \subset \mathbb{F}_q$.

Le résultat d'unicité des corps finis est encore plus fort qu'une simple unicité à isomorphisme près : dans n'importe quelle clôture algébrique de $\overline{\mathbb{F}}_p$, le corps $\mathbb{F}_q$ est unique.

Proposition IV.E.1. Soit $q = p^n$ et $d \geq 1$ un entier. Soit $\overline{\mathbb{F}}_q$ une clôture algébrique de $\mathbb{F}_q$. Il existe une unique extension $\mathbb{F}_q \subset \mathbb{K} \subset \overline{\mathbb{F}}_q$ de degré d sur $\mathbb{F}_q$ et elle est égale au corps $\mathbb{F}_{q^d} = \mathbb{F}_{p^{nd}}$.

Démonstration. Le corps de décomposition de $X^{q^d} - X = X^{p^{nd}} - X$ est égal à $\mathbb{F}_{q^d}$ qui est de degré nd sur $\mathbb{F}_p \subset \overline{\mathbb{F}}_q$. Par multiplicativité des degrés, on en déduit que $[\mathbb{F}_{q^d} : \mathbb{F}_q] = d$. Réciproquement, si une extension est de degré d sur $\mathbb{F}_q$ alors elle est de degré nd sur $\mathbb{F}_p$ et est donc égale à $\mathbb{F}_{q^d}$. ◇

Théorème IV.E.2. Le groupe des automorphismes de $\mathbb{F}_q$, où $q = p^n$, est cyclique d'ordre n. Il est engendré par l'automorphisme de Frobenius $\mathrm{Frob}_{\mathbb{F}_q}$.

Lemme IV.E.3. L'automorphisme de Frobenius de $\mathbb{F}_{p^n}$ est d'ordre n.

Démonstration. Soit d l'ordre de $\varphi = \mathrm{Frob}_{\mathbb{F}_{p^n}}$. Pour tout x, on a donc $\varphi^d(x) = x^{p^d} = x$, donc tous les éléments de $\mathbb{F}_q$ sont racines de $X^{p^d} - X$. Ce polynôme admet au plus p^d racines, donc $p^d \geq p^n \Rightarrow d \geq n$. Mais par ailleurs $\varphi^n(x) = ((x^p)^p \dots)^p = x^{p^n} = x^q = x$ est l'identité, donc $d \leq n$ et finalement $d = n$. ◇

Démontrons maintenant que le groupe engendré par l'automorphisme de Frobenius, qui est cyclique d'ordre n, contient tous les automorphismes de $\mathbb{F}_q$. Nous aurons besoin de quelques lemmes. Ils sont

appliqués ici au cas spécifique des corps finis, mais ils seront grandement généralisés dans le chapitre suivant quand nous travaillerons sur les extensions séparables.

Lemme IV.E.4. Soit $\mathbb{K}(\alpha)$ une extension algébrique monogène d'un corps $\mathbb{K}$, $P = \mathrm{Irr}_{\mathbb{K}}(\alpha)$ le polynôme minimal de α et d le nombre de racines distinctes de P. Soit $\sigma\colon \mathbb{K} \to \mathbb{K}$ un automorphisme. Il existe exactement d automorphismes $\tau\colon \mathbb{K}(\alpha) \to \mathbb{K}(\alpha)$ qui prolongent σ, c'est-à-dire tels que le diagramme suivant commute :

$$\begin{array}{ccc} \mathbb{K} & \hookrightarrow & \mathbb{K}(\alpha) \\ \downarrow f & & \downarrow \tau \\ \mathbb{K} & \hookrightarrow & \mathbb{K}(\alpha) \end{array}$$

Démonstration. Soit $\sigma(P) \in \mathbb{K}[X]$ l'image de P par σ appliqué aux coefficients de P. Tout automorphisme τ est uniquement déterminé par l'image $\tau(\alpha) = \beta$, qui est une racine de $\sigma(P)$, par la formule suivante :

$$x_0 + x_1\alpha + \cdots + x_n\alpha^n \overset{\tau}{\longmapsto} \sigma(x_0) + \sigma(x_1)\beta + \cdots \sigma(x_n)\beta^n.$$

Bien entendu, $\sigma(P)$ a autant de racines que P, donc il y a exactement d prolongements. ◇

En particulier, le nombre de prolongements est inférieur ou égal au degré $[\mathbb{K}(\alpha)\colon \mathbb{K}] = \deg(Irr_{\mathbb{K}}(\alpha))$.

Lemme IV.E.5. Soit $\mathbb{K} \subset \mathbb{L}$ une extension finie et $\sigma\colon \mathbb{K} \to \mathbb{K}$ un automorphisme. Il existe au plus $[\mathbb{L}\colon \mathbb{K}]$ prolongements $\tau\colon \mathbb{L} \to \mathbb{L}$ de σ.

Démonstration. Comme l'extension est finie, on peut écrire $\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_r)$ avec α_i algébrique sur $\mathbb{K}$, $\alpha_{i+1} \notin \mathbb{K}(\alpha_1, \dots, \alpha_i)$. On a donc une tour d'extensions :

$$\mathbb{K} \subset \mathbb{K}(\alpha_1) \subset \mathbb{K}(\alpha_1, \alpha_2) \subset \cdots \subset \mathbb{K}(\alpha_1, \dots, \alpha_r) = \mathbb{L}.$$

Pour $0 \leq i \leq r$, notons $\mathbb{K}_i = \mathbb{K}(\alpha_1, \dots, \alpha_i)$. L'automorphisme σ se prolonge en au plus $[\mathbb{K}_1\colon \mathbb{K}_0]$ automorphismes de $\mathbb{K}_1$, qui se prolongent eux-mêmes chacun en au plus $[\mathbb{K}_2\colon \mathbb{K}_1]$ automorphismes de $\mathbb{K}_2$, etc. Cela produit en fin de compte au plus $\prod_{i=0}^{r-1}[\mathbb{K}_{i+1}\colon \mathbb{K}_i] = [\mathbb{L}\colon \mathbb{K}]$ prolongements. Réciproquement, tout prolongement de σ en un automorphisme de $\mathbb{L}$ se restreint en des automorphismes de $\mathbb{K}_i$, donc il y a bien au total au plus $[\mathbb{L}\colon \mathbb{K}]$ prolongements. ◇

Si $\varphi\colon \mathbb{F}_q \to \mathbb{F}_q$ est un automorphisme, alors pour $k \in \mathbb{F}_p \subset \mathbb{F}_q$, on a $\varphi(k) = k$, car $\varphi(k) = \varphi(1 + \cdots + 1) = \varphi(1) + \cdots + \varphi(1) = 1 + \cdots + 1 = k$. Chaque automorphisme de $\mathbb{F}_q$ est donc un prolongement de l'identité. Par ce qui précède, il y a au plus $\left[\mathbb{F}_q\colon \mathbb{F}_p\right] = n$ prolongements de cet automorphisme. Le sous-groupe engendré par l'automorphisme de Frobenius, qui est de cardinal n, contient donc tous les automorphismes de $\mathbb{F}_q$. ◇

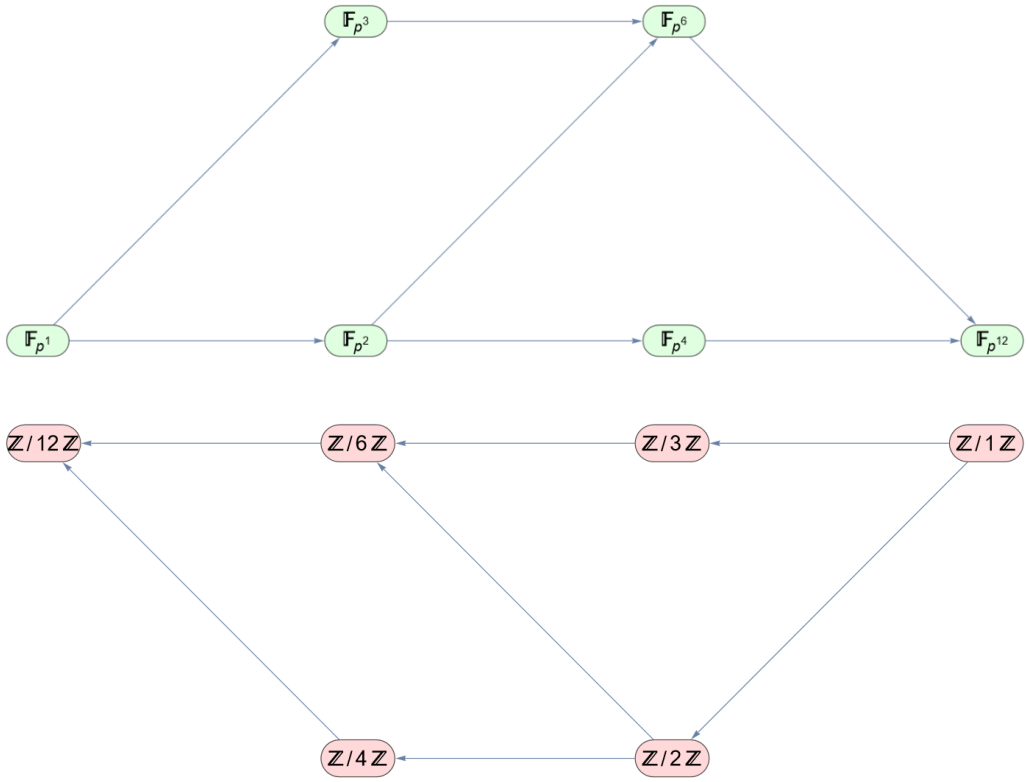
Le groupe des automorphismes de $\mathbb{F}_{p^n}$ est donc cyclique d'ordre n. Ses sous-groupes sont donc des groupes cycliques d'ordre m avec $m|n$. Le « miroir » de ce résultat par la théorie de Galois est le théorème suivant :

Théorème IV.E.6. Soit p un nombre premier et $m, n \geq 1$ des entiers. Dans une clôture algébrique de $\mathbb{F}_p$, le corps $\mathbb{F}_{p^m}$ est contenu dans $\mathbb{F}_{p^n}$ si et seulement si m divise n. Dans ce cas, le groupe des automorphismes de $\mathbb{F}_{p^n}$ qui se restreignent en l'identité sur $\mathbb{F}_{p^m}$ est cyclique d'ordre n/m, et est engendré par $\mathrm{Frob}_{\mathbb{F}_{p^n}}^m$.

Exercice IV.E.7. Démontrer ce théorème ; il n'y a pas de difficultés particulières en utilisant ce qu'on a déjà vu.

Exemple IV.E.8. L'extension $\mathbb{F}_{p^{12}}$ contient six sous-extensions : $\mathbb{F}_p$, $\mathbb{F}_{p^2}$, $\mathbb{F}_{p^3}$, $\mathbb{F}_{p^4}$, $\mathbb{F}_{p^6}$, et $\mathbb{F}_{p^{12}}$ lui-même. Pour $d|12$, la sous-extension $\mathbb{F}_{p^d}$ est l'ensemble des points fixes de $\mathrm{Frob}_{\mathbb{F}_{p^{12}}}^d$. Ces sous-extensions correspondent aux sous-groupes de $\mathbb{Z}/12\mathbb{Z}$, qui est le groupe des automorphismes de $\mathbb{F}_{p^{12}}$ – engendré par l'automorphisme de Frobenius.

Les diagrammes suivants résume comment ces extensions sont reliées et comment elles correspondent aux sous-groupes de $\mathrm{Aut}(\mathbb{F}_{p^{12}}) = \mathbb{Z}/12\mathbb{Z}$:



Chapitre V. Éléments de théorie de Galois

« La symétrie, c'est l'ennui. »

Victor Hugo, *Les Misérables*

Dans ce chapitre, nous allons généraliser l'observation de la fin du chapitre précédent : les sous-extensions de $\mathbb{F}_p \subset \mathbb{F}_{p^n}$ correspondent aux sous-groupes du groupe des automorphismes de $\mathbb{F}_{p^n}$. Nous allons nous concentrer sur les extensions finies ; le cas des extensions infinies est plus délicat.

Section V.A. Extensions normales

On a remarqué que parfois, si $\mathbb{L}$ est le corps de rupture d'un polynôme $P \in \mathbb{K}[X]$, il est possible que P ne soit pas scindé dans $\mathbb{L}$. C'est par exemple le cas de $P = X^3 - 2 \in \mathbb{Q}[X]$: dans le corps de rupture $\mathbb{Q}(\sqrt[3]{2})$, le polynôme P n'est pas scindé car il « manque » toujours des racines (à savoir $j\sqrt[3]{2}$ et $\bar{j}\sqrt[3]{2}$).

Définition V.A.1. Une extension $\mathbb{K} \subset \mathbb{L}$ est *normale* si tout polynôme irréductible de $\mathbb{K}[X]$ qui admet une racine dans $\mathbb{L}$ est scindé dans $\mathbb{L}[X]$.

Exemple V.A.2. Soit $\alpha = \sqrt[3]{2}$. L'extension $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ n'est pas normale. En effet, $X^3 - 2$ y admet une racine, mais il n'est pas scindé. On peut le factoriser comme $(X - \alpha)(X^2 + \alpha X + \alpha^2)$, et $X^2 + \alpha X + \alpha^2$ n'admet pas de racine réelle (et donc certainement pas dans $\mathbb{Q}(\alpha)$), donc il est irréductible pour des raisons de degré. Le théorème suivant implique que $\mathbb{Q} \subset \mathbb{Q}(j, \sqrt[3]{2})$, le corps de décomposition de $X^3 - 2 \in \mathbb{Q}[X]$, est une extension normale.

Théorème V.A.3. Une extension de corps $\mathbb{K} \subset \mathbb{L}$ est finie et normale si et seulement si $\mathbb{L}$ est le corps de décomposition d'un polynôme de $\mathbb{K}[X]$.

Démonstration. Supposons d'abord que $\mathbb{K} \subset \mathbb{L}$ est normale. Comme $[\mathbb{L}:\mathbb{K}] = r < \infty$, on peut choisir une base $(x_1, \dots, x_d)$ de $\mathbb{L}$ comme $\mathbb{K}$-espace vectoriel. L'extension étant normale, chacun des polynômes minimaux $P_i = \mathrm{Irr}_{\mathbb{K}}(x_i)$ est scindé dans $\mathbb{L}$, donc le polynôme $Q = P_1 \dots P_r$ l'est aussi. Comme $\mathbb{L}$ est engendré par les x_i qui sont des racines de Q, c'est donc bien le corps de décomposition de Q.

Réciproquement, supposons que $\mathbb{L} = \mathcal{D}_{\mathbb{K}}(Q)$ pour un certain polynôme $Q \in \mathbb{K}[X]$. Étant donné un polynôme irréductible $P \in \mathbb{K}[X]$ qui admet une racine $x \in \mathbb{L}$, on cherche à montrer qu'il est scindé dans $\mathbb{L}$. Soit $\mathbb{M} = \mathcal{D}_{\mathbb{L}}(P)$ le corps de décomposition de P sur $\mathbb{L}$. Il suffit de montrer que si $y \in \mathbb{M}$ est une autre racine de P alors $y \in \mathbb{L}$.

Chacun des corps $\mathbb{K}(x)$ et $\mathbb{K}(y)$ est un corps de rupture de P sur $\mathbb{K}$, donc il existe un $\mathbb{K}$-isomorphisme $\sigma: \mathbb{K}(x) \to \mathbb{K}(y)$. De plus, $\mathbb{L} = \mathbb{L}(x)$ est un corps de décomposition de Q sur $\mathbb{K}(x)$. L'extension composée $\mathbb{K}(x) \xrightarrow{\sigma} \mathbb{K}(y) \to \mathbb{L}(y)$ est un (autre) corps de décomposition de Q sur $\mathbb{K}(x)$, donc il existe un $\mathbb{K}(x)$-isomorphisme $\tau: \mathbb{L}(x) \to \mathbb{L}(y)$ et donc :

$$[\mathbb{L}:\mathbb{K}(x)] = [\mathbb{L}(x):\mathbb{K}(x)] = [\mathbb{L}(y):\mathbb{K}(x)].$$

Par multiplicativité du degré, on a donc $[\mathbb{L}:\mathbb{K}] = [\mathbb{L}(y):\mathbb{K}]$ et donc $\mathbb{L} = \mathbb{L}(y)$, c'est-à-dire $y \in \mathbb{L}$. ◇

Corollaire V.A.4. Une extension $\mathbb{K} \subset \mathbb{L}$ est normale si et seulement si $\mathbb{L}$ est le corps de décomposition d'une famille (non nécessairement finie) de polynômes de $\mathbb{K}$.

Remarque V.A.5. Si $\mathbb{K} \subset \mathbb{M}$ est une extension normale et si $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ est une sous-extension, alors $\mathbb{L} \subset \mathbb{M}$ est normale (car c'est aussi un corps de décomposition sur $\mathbb{L}$). En revanche, $\mathbb{K} \subset \mathbb{L}$ n'est pas nécessairement normale.

Remarque V.A.6. La composée de deux extensions normales n'est pas toujours normale : par exemple, $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ est normale et $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$ l'est aussi, mais $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2})$ n'est pas normale.

Corollaire V.A.7. Soit $\mathbb{K} \subset \mathbb{L}$ une extension finie et $\overline{\mathbb{K}}$ une clôture algébrique de $\mathbb{K}$. Alors l'extension $\mathbb{K} \subset \mathbb{L}$ est normale si et seulement si tous les $\mathbb{K}$-morphismes $\mathbb{L} \to \overline{\mathbb{K}}$ ont la même image.

Démonstration. Si l'extension $\mathbb{K} \subset \mathbb{L}$ est normale, alors $\mathbb{L} = \mathcal{D}_{\mathbb{K}}(P)$ est le corps de décomposition de $P \in \mathbb{K}[X]$. Si $\sigma : \mathbb{L} \to \overline{\mathbb{K}}$ est un $\mathbb{K}$-morphisme, l'image $\sigma(\mathbb{L})$ est engendrée par les racines de P dans $\overline{\mathbb{K}}$ et ne dépend donc pas de σ.

Réciproquement, supposons que tous les morphismes $\sigma : \mathbb{L} \to \overline{\mathbb{K}}$ ont la même image, disons $\mathrm{im}(\sigma) = \mathbb{L}' \subset \overline{\mathbb{K}}$. Supposons que $Q \in \mathbb{K}[X]$ est irréductible et admet une racine $x \in \mathbb{L}$, et démontrons que Q est scindé dans $\mathbb{L}$. Pour cela, il suffit de démontrer que toute racine $y \in \overline{\mathbb{K}}$ de Q dans la clôture algébrique appartient à $\mathbb{L}'$. Or, chacun des corps $\mathbb{K}(x) \subset \mathbb{L}$ et $\mathbb{K}(y) \subset \overline{\mathbb{K}}$ sont des corps de rupture de Q. Ils sont donc $\mathbb{K}$-isomorphes via $\tau : \mathbb{K}(x) \to \mathbb{K}(y)$. D'après la **Proposition III.B.38**, le $\mathbb{K}$-morphisme $\tau : \mathbb{K}(x) \to \mathbb{K}(y) \to \overline{\mathbb{K}}$ s'étend en un $\mathbb{K}$-morphisme $\bar{\tau} : \mathbb{L} \to \overline{\mathbb{K}}$. Par hypothèse, l'image de $\bar{\tau}$ est $\mathbb{L}'$; mais y appartient à l'image de τ et donc à fortiori à l'image de $\bar{\tau}$, donc $y \in \mathbb{L}'$, comme escompté. ◇

Corollaire V.A.8. Soit $\mathbb{K} \subset \mathbb{L}$ une extension normale finie. Tout automorphisme de $\mathbb{K}$ se prolonge en un automorphisme de $\mathbb{L}$.

Démonstration. Soit $\sigma : \mathbb{K} \to \mathbb{K}$ un automorphisme et soit $\mathbb{L} \subset \overline{\mathbb{L}}$ la clôture algébrique de $\mathbb{L}$. D'après la **Proposition III.B.38**, le morphisme $\mathbb{K} \xrightarrow{\sigma} \mathbb{K} \hookrightarrow \mathbb{L} \hookrightarrow \overline{\mathbb{L}}$ se prolonge en un morphisme $\sigma' : \mathbb{L} \to \overline{\mathbb{L}}$. D'après le corollaire précédent, l'image de σ' a la même image que $\mathbb{K} \hookrightarrow \overline{\mathbb{L}}$, qui est bien sûr $\mathbb{L}$. Donc σ' est bien un automorphisme du corps $\mathbb{L}$. ◇

Proposition/Définition V.A.9. Soit $\mathbb{K} \subset \mathbb{L}$ une extension finie et $\overline{\mathbb{L}}$ la clôture algébrique de $\mathbb{L}$. L'ensemble des extensions $\mathbb{L} \subset \mathbb{M} \subset \overline{\mathbb{L}}$ telles que $\mathbb{K} \subset \mathbb{M}$ est normale est non vide et contient un élément minimal qui est une extension finie de $\mathbb{K}$. On l'appelle la *clôture normale* de $\mathbb{L}$ dans $\overline{\mathbb{L}}$.

Démonstration. Soit $(x_1, \dots, x_r)$ une base de $\mathbb{L}$ vu comme espace vectoriel sur $\mathbb{K}$. Soit $P_i = \mathrm{Irr}_{\mathbb{K}}(x_i) \in \mathbb{K}[X]$ le polynôme minimal de x_i et enfin soit $\mathbb{M}$ le corps engendré les racines de $P_1 \dots P_r$ dans $\overline{\mathbb{L}}$. C'est le corps de décomposition de $Q = P_1 \dots P_r$, donc l'extension $\mathbb{K} \subset \mathbb{M}$ est bien normale. De plus, toute extension normale content $\mathbb{L}$ contient une racine de P_i (à savoir x_i), donc P_i doit y être scindé, et l'extension doit donc contenir toutes les racines de P_i, donc doit contenir le corps $\mathbb{M}$. ◇

Exemple V.A.10. La clôture normale de $\mathbb{Q}(\sqrt{2})$ dans $\mathbb{C}$ est $\mathbb{Q}(\sqrt{2}, j)$.

Section V.B. Extensions séparables

Dans cette section, nous allons étudier un phénomène lié aux racines multiples et propre à la caractéristique non nulle.

§ V.B(a) Polynômes séparables

Définition V.B.1. Soit $\mathbb{K}$ un corps. Un polynôme $P \in \mathbb{K}[X]$ est dit *séparable* si toutes ses racines dans son corps de décomposition sont simples. Dans le cas contraire, P est dit *inséparable*.

Lemme V.B.2. Un polynôme P est séparable si et seulement si $P \wedge P' = 1$ (c'est-à-dire P et sa dérivée sont premiers entre eux).

Démonstration. Le PGCD de P et P' est le même dans $\mathbb{K}[X]$ ou dans $\mathcal{D}_{\mathbb{K}}[X]$. Dans $\mathcal{D}_{\mathbb{K}}[X]$, on peut décomposer $P = \prod_i (X - \alpha_i)$ en produit de facteurs linéaires. Si P est séparable, toutes les racines α_i sont simples et donc aucune n'est racine de P', donc aucun des facteurs irréductibles de P n'est facteur de P'. Si au contraire P est inséparable, alors au moins l'une des racines α_i est également racine de P' et $X - \alpha_i$ est un facteur commun de P et P'. ◇

Corollaire V.B.3. Un polynôme irréductible P est séparable si et seulement si $P' \neq 0$.

Démonstration. Clairement, si $P' = 0$ alors P est inséparable car toutes les racines de P sont racines de P'. Si au contraire $P' \neq 0$, et si P et P' n'étaient pas premiers entre eux, alors on P devrait diviser P', ce qui n'est pas possible car $\deg(P') < \deg(P)$. ◇

Corollaire V.B.4. Un polynôme irréductible $P \in \mathbb{K}[X]$ est inséparable si et seulement si $\mathrm{car}(\mathbb{K}) = p > 0$ et $P \in \mathbb{K}[X^p]$, c'est-à-dire le $k$ième coefficient de P est nul si p ne divise pas k.

Démonstration. Si on écrit $P = a_0 + a_1 X + \cdots a_n X^n$ alors $P' = a_1 + 2a_2 X + \cdots + n a_n X^{n-1}$. Pour que ce polynôme soit nul, il faut que $a_k = 0$ si $k \neq 0$ dans $\mathbb{K}$. Si $\mathrm{car}(\mathbb{K}) = 0$, cela entraîne que $P = a_0$ qui est séparable. Si $\mathrm{car}(\mathbb{K}) = p > 0$ alors il faut que $a_k = 0$ si p ne divise pas k. ◇

Remarque V.B.5. En particulier, les polynômes irréductibles sont toujours séparables en caractéristique nulle.

Proposition V.B.6. Soit $\mathbb{K}$ un corps de caractéristique $p > 0$ et $a \in \mathbb{K}$ un élément qui n'est pas une puissance $p$ième ($\nexists y, y^p = a$). Le polynôme $P = X^p - a$ est irréductible et inséparable.

Démonstration. Soit x une racine de P dans $\mathcal{D}_{\mathbb{K}}(P)$, c'est-à-dire $x^p = a$ (en particulier, $x \notin \mathbb{K}$). On a alors, dans le corps de décomposition :

$$P = X^p - a = X^p - x^p = (X - x)^p.$$

En particulier P est inséparable car x est une racine multiple. Supposons maintenant que $Q \in \mathbb{K}[X]$ est un facteur irréductible unitaire de P dans $\mathbb{K}[X]$. Dans le corps de rupture, on doit avoir $Q = (X - x)^d$ pour $d \leq p$. Comme $x \notin \mathbb{K}$, on a $d \geq 2$, donc Q est inséparable et d est un multiple de p, ce qui entraîne que $d = p$ et le polynôme P est irréductible. ◇

Proposition V.B.7. Soit $P \in \mathbb{K}[X]$ un polynôme irréductible unitaire de degré ≥ 2 qui n'a qu'une seule racine dans son corps de décomposition. Alors $\mathrm{car}(\mathbb{K}) = p > 0$ et il existe un élément $a \in \mathbb{K}$ qui n'est pas une puissance $p$ième et un entier $m \geq 1$ tel que $P = X^{p^m} - a$.

Démonstration. Dans le corps de décomposition, on a $P = (X - \alpha)^d$ avec α l'unique racine et $d = \deg(P) \geq 2$. En particulier, P est inséparable, donc la caractéristique de $\mathbb{K}$ n'est pas nulle et d est divisible par p. Écrivons $d = p^m k$ avec $p \wedge k = 1$. Grâce à la « formule magique », on a $P = \left(X^{p^m} - \alpha^{p^m}\right)^k$ et il nous suffit de montrer que $k = 1$.

Soit $Q = \left(X - \alpha^{p^m}\right)^k$ tel que $P = Q\left(X^{p^m}\right)$. Comme P est irréductible, Q est irréductible aussi. Si k n'était pas égal à 1, le polynôme Q serait donc inséparable et donc son degré $k = \deg(Q)$ serait divisible par p, ce qui est contradictoire. On a donc $k = 1$ et $P = X^{p^m} - \alpha^{p^m}$. ◇

§ V.B(b) Corps parfaits

Définition V.B.8. Un corps $\mathbb{K}$ est *parfait* si tout polynôme irréductible de $\mathbb{K}[X]$ est séparable.

Théorème V.B.9. Un corps $\mathbb{K}$ est parfait si et seulement si l'une des deux conditions suivantes est vérifiée :

- La caractéristique de $\mathbb{K}$ est nulle ; ou bien :
- La caractéristique de $\mathbb{K}$ vaut $p > 0$ et tous les éléments de $\mathbb{K}$ sont des puissances $p$ièmes, c'est-à-dire $\mathbb{K}^p = \mathbb{K}$.

Démonstration. Le cas où $\mathrm{car}(\mathbb{K}) = 0$ est clair d'après les résultats de la section précédente. Supposons donc que $\mathrm{car}(\mathbb{K}) = p > 0$. D'après la section précédente, si $\mathbb{K} \neq \mathbb{K}^p$, alors pour $a \in \mathbb{K} \setminus \mathbb{K}^p$ le polynôme $P = X^p - a$ est irréductible et inséparable. Supposons donc que $\mathbb{K} = \mathbb{K}^p$ et démontrons qu'alors $\mathbb{K}$ est parfait.

Supposons que $P \in \mathbb{K}[X]$ est irréductible et inséparable. Par ce qui précède, on peut écrire :

$$P = a_0 + a_1 X^p + a_2 X^{2p} + \cdots + a_k X^{kp}.$$

Par l'hypothèse $\mathbb{K} = \mathbb{K}^p$, Chacun des coefficients de P est une puissance $p$ième, disons $a_i = b_i^p$. On a alors :

$$\begin{aligned} P &= b_0^p + b_1^p X^p + b_2^p X^{2p} + \cdots + b_k^p X^{kp} \\ &= (b_0 + b_1 X + b_2 X^2 + \cdots + b_k X^k)^p. \end{aligned}$$

Le polynôme P n'est donc finalement pas irréductible, ce qui est contradictoire. ◇

Définition V.B.10. Soit $\mathbb{K}$ un corps de caractéristique $p > 0$. Le corps est parfait si et seulement si son morphisme de Frobenius $\mathrm{Frob}_{\mathbb{K}} : x \mapsto x^p$ est bijectif ; on note alors $x \mapsto x^{1/p}$ son inverse.

Corollaire V.B.11. Tout corps fini est parfait.

Corollaire V.B.12. Tout corps algébriquement clos est parfait.

Démonstration. Si $\mathbb{K}$ est algébriquement clos et de caractéristique $p > 0$, étant donné $a \in \mathbb{K}$ quelconque, $X^p - a$ admet une racine b dans $\mathbb{K}$, donc $a = b^p$ est bien une puissance $p$ième. ◇

Exemple V.B.13. Le corps $\mathbb{F}_p(X)$ n'est pas parfait. Par exemple, le polynôme $Y^p - X \in \mathbb{F}_p(X)[Y]$ est irréductible et inséparable. L'élément $X \in \mathbb{F}_p(X)$ n'est pas une puissance $p$ième.

Exercice V.B.14. Soit $\mathbb{K}$ un corps de caractéristique $p > 0$ et $a \in \mathbb{K} \setminus \mathbb{K}^p$.

- Démontrer que $X^{p^m} - a$ est irréductible et inséparable pour tout $m \geq 1$.
- En déduire que si $\mathbb{K} \subset \mathbb{L}$ est une extension *finie* et que $\mathbb{L}$ est parfait, alors $\mathbb{K}$ est parfait.

Remarque V.B.15. Un sous-corps d'un corps parfait n'est pas toujours parfait. Par exemple, $\mathbb{F}_p(X)$ est contenu dans sa clôture algébrique qui est parfaite.

§ V.B(c) Extensions séparables

Définition V.B.16. Soit $\mathbb{K} \subset \mathbb{L}$ une extension de corps et $a \in \mathbb{L}$ un élément algébrique sur $\mathbb{K}$. On dit que a est *séparable* sur $\mathbb{K}$ si son polynôme minimal $\mathrm{Irr}_{\mathbb{K}}(a)$ est séparable.

Définition V.B.17. Une extension $\mathbb{K} \subset \mathbb{L}$ est *séparable* si tout élément de $\mathbb{L}$ est séparable sur $\mathbb{K}$.

Remarque V.B.18. Une extension séparable est donc algébrique. Si $\mathrm{car}(\mathbb{K}) = 0$, toutes ses extensions algébriques sont séparables.

Proposition V.B.19. Un corps $\mathbb{K}$ est parfait si et seulement si toutes ses extensions algébriques sont séparables.

Démonstration. Si $\mathbb{K}$ est parfait et $\mathbb{L}$ est une extension algébrique, le polynôme minimal de n'importe quel élément $a \in \mathbb{L}$ est irréductible et donc séparable (car $\mathbb{K}$ est parfait). Réciproquement, supposons que toute extension algébrique de $\mathbb{K}$ est séparable. Supposons que $\mathrm{car}(\mathbb{K}) = p > 0$ (le cas de la caractéristique nulle est évident) et soit $a \in \mathbb{K}$. Si a n'était pas une puissance $p$ième, alors le polynôme $P = X^p - a$ serait irréductible et inséparable. Mais dans le corps de rupture $\mathbb{K}(\alpha)$ de P, qui est une extension algébrique de $\mathbb{K}$, le polynôme minimal de α est P qui est inséparable, une contradiction. ◇

Soit $\sigma\colon \mathbb{K} \to \mathbb{K}(\alpha)$ une extension algébrique monogène et $\iota\colon \mathbb{K} \to \Omega$ une extension algébriquement close de $\mathbb{K}$. On a vu (**Proposition III.B.38**) qu'il existe un prolongement $\tau\colon \mathbb{K}(\alpha) \to \overline{\mathbb{K}}$ de σ, c'est-à-dire un morphisme tel que $\tau \circ \sigma = \iota$, et que le nombre de prolongements possibles est égal au nombre de racines distinctes du polynôme minimal $\mathrm{Irr}_{\mathbb{K}}(\alpha)$.

Plus généralement, on obtient (simplement en se servant du fait que deux clôtures algébriques de $\mathbb{K}$ sont $\mathbb{K}$-isomorphes) :

Proposition/Définition V.B.20. Soit $\sigma\colon \mathbb{K} \to \mathbb{L}$ une extension et Ω une extension algébriquement close de $\mathbb{K}$. Le nombre de prolongements $\tau\colon \mathbb{L} \to \Omega$ de σ ne dépend pas de Ω. On note ce nombre $[\mathbb{L}\colon \mathbb{K}]_s$ et on l'appelle le *degré séparable* de l'extension.

Exemple V.B.21. Le degré séparable de l'extension $\mathbb{R} \subset \mathbb{C}$ vaut $[\mathbb{C}\colon \mathbb{R}]_s = 2$. Les deux prolongements possibles $\tau\colon \mathbb{C} \to \overline{\mathbb{R}} = \mathbb{C}$ sont l'identité et la conjugaison complexe, caractérisés respectivement par $\tau(i) = i$ et $\tau(i) = -i$ et étendus en $\mathbb{R}$-morphismes.

Exemple V.B.22. Soit $\mathbb{Q}(\alpha)$ le corps de rupture de $X^3 - 2$ (c'est-à-dire $\alpha^3 = 2$). Le degré séparable $[\mathbb{Q}(\alpha)\colon \mathbb{Q}]_s$ vaut 3 et les trois prolongements possibles $\tau\colon \mathbb{Q}(\alpha) \to \overline{\mathbb{Q}} \subset \mathbb{C}$ sont respectivement caractérisés par $\tau(\alpha) = \sqrt[3]{2}$, $\tau(\alpha) = j\sqrt[3]{2}$ et $\tau(\alpha) = j^2\sqrt[3]{2}$ (où $j = \exp(2i\pi/3)$ est une racine cubique primitive de l'unité).

On remarque que dans chacun de ces deux cas, le degré séparable est égal au degré de l'extension. Ce n'est pas toujours le cas :

Exemple V.B.23. Soit p un nombre premier, $\mathbb{L} = \mathbb{F}_p(X)$ le corps des fractions rationnelles à coefficients dans $\mathbb{F}_p$, et $\mathbb{K} = \mathbb{L}^p = \mathbb{F}_p(X^p)$ le sous-corps des fractions qui ne font intervenir que les puissances de X de la forme X^{pk}. Alors le degré séparable $\left[\mathbb{F}_p(X)\colon \mathbb{F}_p(X^p)\right]_s$ vaut 1. En effet, soit $\iota\colon \mathbb{F}_p(X^p) \to \overline{\mathbb{L}}$ une clôture algébrique et $\tau\colon F_p(X) \to \overline{\mathbb{F}_p(X^p)}$ un prolongement de $\sigma\colon \mathbb{F}_p(X^p) \to \mathbb{F}_p(X)$, alors on doit avoir $\tau(X) = \tau\left((X^p)^{1/p}\right) = \tau(X^p)^{1/p} = \sigma(X^p)^{1/p}$ (le morphisme de Frobenius est injectif) et donc τ est uniquement déterminé.

Mais bien sûr, $\left[\mathbb{F}_p(X)\colon \mathbb{F}_p(X^p)\right]$ n'est pas égal à 1, car les deux corps sont différents, donc le degré séparable n'est pas égal au degré de l'extension. En fait, on a $\left[\mathbb{F}_p(X)\colon \mathbb{F}_p(X^p)\right] = p \geq 2$ et une base de $\mathbb{F}_p(X)$ comme $\mathbb{F}_p(X^p)$-espace vectoriel est donnée par $\{1, X, \dots, X^{p-1}\}$.

Théorème V.B.24. Soit $\mathbb{K} \subset \mathbb{L}$ une extension finie de corps. Alors $[\mathbb{L}\colon \mathbb{K}]_s \leq [\mathbb{L}\colon \mathbb{K}]$ et l'égalité est atteinte si et seulement si l'extension est séparable.

Lemme V.B.25. Le degré séparable est multiplicatif : si $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ est une suite d'extensions de corps,

$$[\mathbb{M}:\mathbb{K}]_s = [\mathbb{M}:\mathbb{L}]_s \cdot [\mathbb{L}:\mathbb{K}]_s.$$

Démonstration. Soit $\Omega = \overline{\mathbb{M}}$, soit $m = [\mathbb{M}:\mathbb{L}]_s$ et soit $n = [\mathbb{L}:\mathbb{K}]_s$. Il y a n prolongements $\sigma_1, \dots \sigma_n : \mathbb{L} \to \Omega$ de $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M} \subset \Omega$, et chacun de ces prolongements σ_i se prolonge en m morphismes $\tau_{i,1}, \dots, \tau_{i,m} : \mathbb{M} \to \Omega$, ce qui produit nm prolongements distincts. Réciproquement, tout prolongement $\tau : \mathbb{M} \to \Omega$ de $\mathbb{K} \subset \Omega$ fait partie de cette liste (car il se restreint d'abord un un prolongement $\tau|_{\mathbb{L}} : \mathbb{L} \to \Omega$ qui est l'un des σ_i). ◇

Démonstration du théorème. Comme l'extension est finie, on peut écrire $\mathbb{L}$ comme l'extension finale d'une suite d'extensions monogènes, avec $\mathbb{K}_{i+1} = \mathbb{K}_i(\alpha_i)$:

$$\mathbb{K} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_r = \mathbb{L}.$$

Par multiplicativité, il suffit donc de démontrer l'inégalité pour les extensions monogènes. D'après la **Proposition III.B.38**, le nombre de prolongements $\mathbb{K}_{i+1} \to \Omega$ d'un morphisme $\mathbb{K}_i \to \Omega$ (où Ω est algébriquement clos) est égal au nombre de racines distinctes du polynôme minimal $P_i \in \mathbb{K}_i[X]$ de α_i. Le nombre de racines distinctes, qui vaut donc $[\mathbb{K}_{i+1}:\mathbb{K}_i]_s$ est inférieur ou égal à $\deg(P_i) = [\mathbb{K}_{i+1}:\mathbb{K}_i]$, et l'égalité est atteinte si et seulement si $\alpha_i \in \mathbb{K}_{i+1}$ est séparable sur $\mathbb{K}_i$. Cela montre donc déjà l'inégalité.

Si l'extension $\mathbb{K} \subset \mathbb{L}$ est séparable alors chaque α_i est séparable sur $\mathbb{K}$ et donc a fortiori séparable sur $\mathbb{K}_i$ (car son polynôme minimal sur $\mathbb{K}_i$ divise son polynôme minimal sur $\mathbb{K}$) donc on a bien l'égalité à chaque étape. Réciproquement, si $[\mathbb{L}:\mathbb{K}]_s = [\mathbb{L}:\mathbb{K}]$, montrons que tout $x \in \mathbb{L}$ est séparable. On a montré que $[\mathbb{L}:\mathbb{K}(x)]_s \leq [\mathbb{L}:\mathbb{K}(x)]$ et $[\mathbb{K}(x):\mathbb{K}]_s \leq [\mathbb{K}(x):\mathbb{K}]$. Par multiplicativité, ces deux inégalités sont en fait des égalités, en particulier $[\mathbb{K}(x):\mathbb{K}]_s = [\mathbb{K}(x):\mathbb{K}]$ et donc toutes les racines du polynôme minimal de x sont distinctes et x est séparable sur $\mathbb{K}$. ◇

Corollaire V.B.26. Si $\mathbb{L} = \mathbb{K}(x_1, \dots, x_n)$ avec les x_i séparables sur $\mathbb{K}$, alors l'extension $\mathbb{K} \subset \mathbb{L}$ est séparable.

Théorème V.B.27. Soit $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ une suite d'extensions de corps. Si $\mathbb{K} \subset \mathbb{L}$ est séparable et si $x \in \mathbb{M}$ est séparable sur $\mathbb{L}$, alors x est séparable sur $\mathbb{K}$.

Démonstration. Soit $P = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{L}[X]$ le polynôme minimal de x sur $\mathbb{L}$ et soit $\mathbb{L}' = \mathbb{K}(a_0, \dots, a_n)$. L'extension $\mathbb{L}'$ est séparable et finie sur $\mathbb{K}$, donc $[\mathbb{L}':\mathbb{K}]_s = [\mathbb{L}':\mathbb{K}]$. De plus, x est séparable sur $\mathbb{L}'$, donc $[\mathbb{L}'(x):\mathbb{L}']_s = [\mathbb{L}'(x):\mathbb{L}']$. Par multiplicativité, on en déduit que $[\mathbb{L}'(x):\mathbb{K}]_s = [\mathbb{L}'(x):\mathbb{K}]$, donc l'extension $\mathbb{L}'(x)$ est séparable sur $\mathbb{K}$ et donc finalement x est séparable sur $\mathbb{K}$. ◇

Corollaire V.B.28. Soit $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ une suite d'extensions de corps. L'extension $\mathbb{K} \subset \mathbb{M}$ est séparable si et seulement si $\mathbb{K} \subset \mathbb{L}$ et $\mathbb{L} \subset \mathbb{M}$ sont séparables.

Corollaire/Définition V.B.29. Soit $\mathbb{K} \subset \mathbb{L}$ une extension de corps. L'ensemble suivant forme un sous-corps de $\mathbb{L}$ qui est une extension séparable de $\mathbb{K}$:

$$\mathbb{L}' = \{ x \in \mathbb{L} \mid x \text{ est séparable sur } \mathbb{K} \}.$$

On l'appelle la *clôture séparable* de $\mathbb{K}$ dans $\mathbb{L}$. La clôture séparable de $\mathbb{K}$ dans sa clôture algébrique $\overline{\mathbb{K}}$ s'appelle la *clôture séparable* de $\mathbb{K}$. Elle est notée $\overline{\mathbb{K}}^s$.

Démonstration. Si x, y sont des éléments de $\mathbb{L}$ ($y \neq 0$) qui sont séparables sur $\mathbb{K}$, l'extension $\mathbb{K}(x,y)$ est séparable et donc $x-y$ et x/y sont séparables sur $\mathbb{K}$. L'ensemble $\mathbb{L}'$ est donc un sous-corps de $\mathbb{L}$. Il est clair qu'elle est séparable sur $\mathbb{K}$. ◇

Remarque V.B.30. Un corps $\mathbb{K}$ est parfait si et seulement si $\overline{\mathbb{K}} = \overline{\mathbb{K}}^s$. Tout élément de $\overline{\mathbb{K}} \setminus \overline{\mathbb{K}}^s$ est inséparable sur $\overline{\mathbb{K}}^s$ et donc sur $\mathbb{K}$.

Remarque V.B.31. Une extension séparable de $\overline{\mathbb{K}}^s$ est nécessairement triviale.

Section V.C. Théorème de l'élément primitif

Dans cette section, nous allons tenter de détecter quand une extension d'un corps $\mathbb{K}$ est monogène, c'est-à-dire de la forme $\mathbb{K}(\alpha)$, engendrée par un seul élément α (appelé élément primitif).

Exemple V.C.1. Est-ce que $\mathbb{L} = \mathbb{Q}(\sqrt[3]{2}, j)$, le corps de décomposition de $X^3 - 2 \in \mathbb{Q}[X]$, est une extension monogène de $\mathbb{Q}$? La réponse est oui ! On a $\mathbb{L} = \mathbb{Q}(\alpha)$ avec $\alpha = \sqrt[3]{2} + j$. Il est clair que $\mathbb{Q}(\alpha) \subset \mathbb{L}$. Réciproquement, on doit montrer que $\sqrt[3]{2}$ et j appartiennent à $\mathbb{Q}(\alpha)$. Un long calcul (ou la fonction `ToNumberField` de Mathematica…) donne :

$$\sqrt[3]{2} = 2 + \alpha - \frac{2\alpha^2}{3} + \frac{2\alpha^3}{3} + \frac{\alpha^4}{3} + \frac{2\alpha^5}{9},$$
$$j = -2 + \frac{2\alpha^2}{3} - \frac{2\alpha^3}{3} - \frac{\alpha^4}{3} - \frac{2\alpha^5}{9}.$$

Exemple V.C.2. Soit $\mathbb{L} = \mathbb{F}_p(X,Y)$ le corps des fractions rationnelles à coefficients dans $\mathbb{F}_p$, et soit $\mathbb{K} = \mathbb{L}^p = \mathbb{F}_p(X^p, Y^p)$ le sous-corps engendré par X^p et Y^p. Est-ce que l'extension $\mathbb{K} \subset \mathbb{L}$ est monogène ?

La réponse est non. L'extension $\mathbb{K} \subset \mathbb{L}$ est finie et son degré vaut $[\mathbb{L}:\mathbb{K}] = p^2$ (une base est $\{X^i Y^j\}_{i,j=0}^{p-1}$). Cependant, si $Q \in \mathbb{L} \setminus \mathbb{K}$ est une fraction rationnelle, sa puissance $p$ième Q^p appartient à $\mathbb{K}$ d'après la formule magique, donc le polynôme minimal de Q sur $\mathbb{K}$, $\mathrm{Irr}_{\mathbb{K}}(Q) \in \mathbb{K}[T]$ est un diviseur de $T^p - Q^p \in \mathbb{K}[T]$. Son degré $[\mathbb{K}(Q):\mathbb{K}] = \deg(\mathrm{Irr}_{\mathbb{K}}(Q))$ est donc $\leq p$, et par suite $\mathbb{K}(Q) \neq \mathbb{L}$, quel que soit $Q \in \mathbb{L}$. L'extension $\mathbb{L}$ n'est donc pas monogène : il faut au moins deux générateurs pour l'engendrer.

Le critère suivant ramène l'étude de la recherche d'un générateur (un élément « primitif ») à une question sur la séparabilité de l'extension.

Théorème V.C.3 (de l'élément primitif). Soit $\mathbb{K} \subset \mathbb{L}$ une extension finie de corps. Si on peut écrire $\mathbb{L} = \mathbb{K}(\alpha, \beta_1, \dots, \beta_n)$ avec les β_i séparables sur $\mathbb{K}$, alors il existe $\gamma \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}(\gamma)$.

Corollaire V.C.4. Toute extension finie et séparable est monogène.

Corollaire V.C.5. Si un corps est parfait alors toutes ses extensions finies sont monogènes.

Remarque V.C.6. Même si on sait qu'une extension est monogène, trouver un élément primitif, ou l'ensemble de ses éléments primitifs, n'est pas toujours facile. Par exemple dans $\mathbb{F}_{17^3} = \mathbb{F}_{17}[X]/(X^3 + X + 14)$, l'élément $\alpha = [X]$ est primitif, mais $\alpha^2 + 7\alpha + 6$ est également primitif. Il fallait le deviner !

Démonstration du théorème. Si $\mathbb{K}$ est fini, alors $\mathbb{L}$ aussi et son groupe des unités $\mathbb{L}^\times$ est cyclique. Si γ engendre $\mathbb{L}^\times$ alors on a bien $\mathbb{L} = \mathbb{K}(\gamma)$. On peut donc supposer $\mathbb{K}$ infini. Par récurrence, il suffit de

traiter le cas $n = 1$ et on peut supposer que $\mathbb{L} = \mathbb{K}(\alpha, \beta)$ avec y séparable sur $\mathbb{K}$. Notons $P = \mathrm{Irr}_{\mathbb{K}}(\alpha)$ et $Q = \mathrm{Irr}_{\mathbb{K}}(\alpha)$. Dans la clôture algébrique $\overline{\mathbb{L}}$, on a :

$$P = \prod_{i=1}^{r}(X - \alpha_i), \qquad Q = \prod_{j=1}^{s}(X - \beta_j).$$

Quitte à échanger les racines, $\alpha_1 = \alpha$ et $\beta_1 = \beta$. De plus, β étant séparable, les racines β_j sont deux à deux distinctes. L'idée est de chercher l'élément primitif γ sous la forme $\alpha + u\beta$ avec $u \in \mathbb{K}$. Comme $\mathbb{K}$ est infini, il existe un élément $u \in \mathbb{K}$ tel que :

$$\forall i \geq 1, \forall j \geq 2, \qquad u \neq \frac{\alpha - \alpha_i}{\beta_j - \beta}.$$

Soit $\gamma \coloneqq \alpha + u\beta$. On trouve donc :

$$P(\gamma - u\beta) = P(\alpha) = 0, \qquad \forall j \geq 2, P\big(\gamma - u\beta_j\big) \neq 0.$$

Le PGCD des polynômes $P(\gamma - uX)$ et Q dans la clôture algébrique est donc $X - \beta$, car β est leur unique racine commune et β étant séparable, c'est une racine simple de son polynôme minimal. Mais le PGCD ne dépend pas de l'extension, et les deux polynômes sont à coefficients dans $\mathbb{K}(\gamma)$, donc leur PGCD est aussi à coefficients dans $\mathbb{K}(\gamma)$ et donc $\beta \in \mathbb{K}(\gamma)$. On obtient donc par suite $\alpha = \gamma - u\beta \in \mathbb{K}(\gamma)$ et donc finalement $\mathbb{K}(\alpha, \beta) = \mathbb{K}(\gamma)$. ◇

Le résultat suivant est bien utile :

Théorème V.C.7. Soit $\mathbb{K} \subset \mathbb{L}$ une extension finie. L'extension est monogène si et seulement s'il n'existe qu'un nombre fini de corps intermédiaires entre $\mathbb{K}$ et $\mathbb{L}$.

Démonstration. Si $\mathbb{K}$ est fini, alors il est parfait donc toutes ses extensions finies (en particulier $\mathbb{L}$) sont monogènes. De plus $\mathbb{L}$ est lui-même un corps fini donc il n'a qu'un nombre fini de sous-corps (et a fortiori de sous-corps contenant $\mathbb{K}$). On peut donc supposer que $\mathbb{K}$ est infini (et donc $\mathbb{L}$ aussi).

Supposons pour commencer que $\mathbb{L} = \mathbb{K}(\alpha)$ est monogène. Soit $P = \mathrm{Irr}_{\mathbb{K}}(\alpha) \in \mathbb{K}[X]$ le polynôme minimal de α sur $\mathbb{K}$. Si $\mathbb{M}$ est un corps intermédiaire entre $\mathbb{K}$ et $\mathbb{L}$, alors le polynôme minimal $P_M = \mathrm{Irr}_{\mathbb{M}}(\alpha) \in \mathbb{M}[X]$ de α sur $\mathbb{M}$ divise (dans $\mathbb{M}[X]$ et a fortiori dans $\mathbb{L}[X]$) le polynôme P. Or l'anneau $\mathbb{L}[X]$ est factoriel, donc P n'a qu'un nombre fini de diviseurs unitaires. On obtient ainsi une application :

$$\psi\colon \{\text{corps intermédiaires } \mathbb{K} \subset \cdots \subset \mathbb{L}\} \to \{\text{diviseurs unitaires de } P \text{ dans } \mathbb{L}[X]\},$$
$$\mathbb{M} \mapsto P_{\mathbb{M}} = \mathrm{Irr}_{\mathbb{M}}(\alpha).$$

Il suffit de montrer que cette application est injective. Or, on peut reconstruire $\mathbb{M}$ à partir de $P_{\mathbb{M}}$ (c'est-à-dire définir une rétraction de ψ qui est donc injective). En effet, si on note $\mathbb{M}' \subset \mathbb{M}$ la sous-$\mathbb{K}$-extension de $\mathbb{L}$ engendrée par les coefficients de $P_{\mathbb{M}}$, alors $P_{\mathbb{M}}$ est irréductible dans $\mathbb{M}'[X]$ donc c'est le polynôme minimal de α sur $\mathbb{M}'$. On en déduit donc que :

$$[\mathbb{L}\colon \mathbb{M}] = [\mathbb{M}(\alpha)\colon \mathbb{M}] = \deg(P_{\mathbb{M}}) = [\mathbb{M}'(\alpha)\colon \mathbb{M}'] = [\mathbb{L}\colon \mathbb{M}'].$$

Comme $\mathbb{M} \subset \mathbb{M}'$, on en déduit que $\mathbb{M} = \mathbb{M}'$ par multiplicativité du degré.

Démontrons maintenant la réciproque du théorème. Supposons que $\mathbb{K} \subset \mathbb{L}$ n'admet qu'un nombre fini de corps intermédiaires. Comme l'extension est finie, on peut écrire $\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_n)$ et par récurrence on voit qu'il suffit de traiter le cas $n = 2$, c'est-à-dire $\mathbb{L} = \mathbb{K}(\alpha, \beta)$. Par le principe des

tiroirs, comme $\mathbb{K}$ est infini mais que $\mathbb{L}$ n'a qu'un nombre fini de sous-extensions, il existe deux éléments $u \neq v \in \mathbb{K}$ tels que $\mathbb{K}(\alpha + u\beta) = \mathbb{K}(\alpha + v\beta)$.

Or, on peut réécrire α et β de la façon suivante :

$$\beta = \frac{(\alpha + v\beta) - (\alpha + u\beta)}{v - u}, \qquad \alpha = (\alpha + u\beta) - u\beta.$$

Cela démontre donc que $\alpha, \beta \in \mathbb{K}(\alpha + u\beta) = \mathbb{K}(\alpha + v\beta)$ et donc finalement que $\mathbb{L} = \mathbb{K}(\alpha + u\beta)$ est bien monogène. ◇

Section V.D. Correspondance de Galois

§ V.D(a) Groupe de Galois

On arrive maintenant à la définition fondamentale de ce chapitre. Rappelons que si $\mathbb{K} \subset \mathbb{L}, \mathbb{L}'$ sont des extensions de corps, on dit qu'un (iso)morphisme $\sigma\colon \mathbb{L} \to \mathbb{L}'$ est un $\mathbb{K}$-(iso)morphisme si la restriction $\sigma|_{\mathbb{K}}$ de σ à $\mathbb{K}$ est l'identité. On dit que c'est un $\mathbb{K}$-endomorphisme/automorphisme si $\mathbb{L} = \mathbb{L}'$. On aura quelquefois besoin de la notation suivante :

Définition V.D.1. Soit $\mathbb{K} \subset \mathbb{L}, \mathbb{L}'$ deux $\mathbb{K}$-extensions. On note $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \mathbb{L}')$ l'ensemble des $\mathbb{K}$-morphismes $\mathbb{L} \to \mathbb{L}'$. On note de plus $\mathrm{End}_{\mathbb{K}}(\mathbb{L}) = \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \mathbb{L})$ l'ensemble des endomorphismes et enfin $\mathrm{Aut}_{\mathbb{K}}(\mathbb{L}) \subset \mathrm{End}_{\mathbb{K}}(\mathbb{L})$ l'ensemble des automorphismes.

Définition V.D.2. Soit $\mathbb{K} \subset \mathbb{L}$ une extension de corps. Le *groupe de Galois* de l'extension, noté $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$, est le groupe $\mathrm{Aut}_{\mathbb{K}}(\mathbb{L})$ des $\mathbb{K}$-automorphismes de $\mathbb{L}$.

Exemple V.D.3. Soit $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})$. Une base de $\mathbb{C}$ sur $\mathbb{R}$ étant donnée par $\{1, i\}$, l'automorphisme σ est entièrement déterminé par $\sigma(i)$. Comme $\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1$, on a $\sigma(i) = \pm i$. Le groupe de Galois a donc deux éléments : l'identité (caractérisée par $\sigma(i) = i$) et la conjugaison complexe (caractérisée par $\sigma(i) = -i$). On remarque que :

$$[\mathbb{C}\colon \mathbb{R}] = 2 = |\mathrm{Gal}(\mathbb{C}/\mathbb{R})|.$$

Exemple V.D.4. Soit $\sigma \in \mathrm{Gal}\left(\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}\right)$. Comme précédemment, σ est déterminé par $\sigma\left(\sqrt[3]{2}\right)$. Comme on a $\sigma\left(\sqrt[3]{2}\right)^3 = 2$ et que la seule racine de $X^3 - 2$ dans le corps $\mathbb{Q}\left(\sqrt[3]{2}\right)$ est $\sqrt[3]{2}$, c'est que σ est l'identité. Le groupe de Galois de l'extension est donc trivial :

$$\left|\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}\right)\right| = 1 < \left[\mathbb{Q}\left(\sqrt[3]{2}\right)\colon \mathbb{Q}\right].$$

Exercice V.D.5. Déterminer $\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{3}, \sqrt{2}\right)/\mathbb{Q}\right)$ et $\mathrm{Gal}(\mathbb{R}/\mathbb{Q})$.

Exemple V.D.6. Soit $\mathbb{L} = \mathbb{F}_p(X)$ et $\mathbb{K} = \mathbb{F}_p(X^p)$. On rappelle que $[\mathbb{L}\colon \mathbb{K}] = p$ avec une base donnée par $\{1, X, \dots, X^{p-1}\}$ et que $[\mathbb{L}\colon \mathbb{K}]_s = 1$. Si $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$, et si $\iota\colon \mathbb{L} \hookrightarrow \overline{\mathbb{L}}$ est le plongement dans la clôture algébrique, alors $\iota \circ \sigma$ est un prolongement de $\mathbb{K} \subset \mathbb{L} \subset \overline{\mathbb{L}}$. Comme le degré séparable vaut 1, ce prolongement est unique, donc σ est l'identité et on a :

$$|\mathrm{Gal}(\mathbb{L}/\mathbb{K})| = 1 = [\mathbb{L}\colon \mathbb{K}]_s < [\mathbb{L}\colon \mathbb{K}].$$

Ces (in)égalités sont des faits généraux, comme indiqué par le théorème suivant :

Théorème V.D.7. Soit $\mathbb{K} \subset \mathbb{L}$ une extension finie. On a la suite d'inégalités suivante :

$$|\mathrm{Gal}(\mathbb{L}/\mathbb{K})| \leq [\mathbb{L}\colon \mathbb{K}]_s \leq [\mathbb{L}\colon \mathbb{K}].$$

De plus, la première égalité est atteinte si et seulement l'extension est normale. La seconde égalité est atteinte si et seulement l'extension est séparable.

Démonstration. La seconde inégalité, et le cas d'égalité correspondant, sont exactement le contenu du **Théorème IV.C.1**. Nous devons seulement démontrer la première inégalité et le cas d'égalité.

Soit $\overline{\mathbb{L}}$ la clôture algébrique de $\mathbb{L}$. Par définition, $[\mathbb{L}:\mathbb{K}]_s$ est le cardinal de $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\overline{\mathbb{L}})$. Le groupe de Galois $G = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ agit à droite sur $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\overline{\mathbb{L}})$ par pré-composition :

$$\forall g \in G, \qquad \forall \sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\overline{\mathbb{L}}), \qquad \sigma \cdot g \coloneqq \sigma \circ g \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\Omega).$$

Cette action est libre : si $\sigma \circ g = \sigma$, comme σ est injectif (c'est un morphisme de corps) on doit avoir $g = \mathrm{id}_{\mathbb{L}}$. Cela montre donc que $|G| \leq [\mathbb{L}:\mathbb{K}]_s$. L'égalité est atteinte si et seulement si l'action est transitive. Le contenu du lemme suivant nous indique quand cela se produit :

Lemme V.D.8. L'action de G sur $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\overline{\mathbb{L}})$ est transitive si et seulement si tous les éléments de $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\overline{\mathbb{L}})$ ont la même image dans $\overline{\mathbb{L}}$.

Démonstration. Supposons pour commencer que l'action est transitive et soit $\sigma,\sigma' \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\Omega)$. Par transitivité, il existe $g \in G$ tel que $\sigma' = \sigma \cdot g = \sigma \circ g$. Comme g est un automorphisme, il est clair que $\mathrm{im}(\sigma') = \mathrm{im}(\sigma)$.

Réciproquement, supposons que tous les éléments de $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\Omega)$ ont la même image. Soit $\sigma,\sigma' \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\Omega)$ deux morphismes, qui vérifient donc $\sigma(\mathbb{L}) = \sigma'(\mathbb{L}) = \mathbb{M}$. On cherche $g:\mathbb{L}\to\mathbb{L}$ tel que $\sigma' = \sigma \circ g$. Or, $\sigma:\mathbb{L}\to\mathbb{M} = \sigma(\mathbb{L})$ est un $\mathbb{K}$-isomorphisme, dont on note l'inverse $\tau:\mathbb{M}\to\mathbb{L}$. La composée $g \coloneqq \tau \circ \sigma'$ est bien définie (car $\sigma'(\mathbb{L}) = \mathbb{M}$ aussi), c'est un $\mathbb{K}$-automorphisme de $\mathbb{L}$, et il vérifie bien $\sigma' = \sigma \circ g$. ◇

Démonstration du théorème. Il suffit désormais d'invoquer le **Corollaire V.A.7** pour conclure la démonstration du théorème. ◇

Remarque V.D.9. On peut en fait démontrer que $|\mathrm{Gal}(\mathbb{L}/\mathbb{K})|$ divise $[\mathbb{L}:\mathbb{K}]_s$. La démonstration dépasse légèrement le cadre de ce cours.

Remarque V.D.10. Calculer le groupe de Galois d'une extension n'est pas toujours facile. Par exemple, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ est un objet assez mystérieux !

§ V.D(b) Extensions galoisiennes

Définition V.D.11. Une extension $\mathbb{K} \subset \mathbb{L}$ est dite *galoisienne* si elle est normale et séparable.

D'après le théorème précédent, une extension finie est galoisienne si et seulement si l'ordre de son groupe de Galois est égal à son degré.

Remarque V.D.12. Si $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ est une suite d'extensions de corps et que $\mathbb{K} \subset \mathbb{M}$ est galoisienne, alors $\mathbb{L} \subset \mathbb{M}$ est aussi galoisienne. De plus, $\mathrm{Gal}(\mathbb{M}/\mathbb{L})$ est un sous-groupe de $\mathrm{Gal}(\mathbb{M}/\mathbb{K})$, car si un automorphisme est trivial sur $\mathbb{L}$, il l'est à fortiori sur $\mathbb{K}$. En revanche, il est possible que $\mathbb{K} \subset \mathbb{L}$ ne soit pas galoisienne : elle est toujours séparable, mais peut ne pas être normale.

Remarque V.D.13. Par le théorème de l'élément primitif, une extension finie galoisienne est monogène.

Le théorème suivant est analogue au **Théorème V.A.3** :

Théorème V.D.14. Soit $\mathbb{K} \subset \mathbb{L}$ une extension finie. Elle est galoisienne si et seulement si $\mathbb{L}$ est le corps de décomposition d'un polynôme séparable de $\mathbb{K}[X]$.

Démonstration. Si $\mathbb{L} = \mathcal{D}_{\mathbb{K}}(Q)$ avec Q séparable, alors l'extension est normale par le **Théorème V.A.3**. Elle est de plus engendrée par les racines de Q qui sont séparables, donc elle est elle-même séparable.

Réciproquement, supposons $\mathbb{K} \subset \mathbb{L}$ galoisienne. Comme elle est finie, on peut écrire $\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_r)$. Soit $P_i = \mathrm{Irr}_{\mathbb{K}}(\alpha_i)$ le polynôme minimal de α_i sur $\mathbb{K}$. Comme l'extension est galoisienne, chacun des P_i est scindé à racines simples dans $\mathbb{L}$. Leur PPCM, $Q = P_1 \vee \dots \vee P_r$, est donc également scindé à racines simples (donc séparable), et $\mathbb{L}$ est le corps de décomposition de Q. ◇

Étant donnée une extension finie galoisienne $\mathbb{K} \subset \mathbb{L}$ de groupe de Galois G, on a $\mathbb{L} = \mathcal{D}_{\mathbb{K}}(P)$ avec $P \in \mathbb{K}[X]$ séparable. Si $n = \deg(P)$, le polynôme P a n racines distinctes et chaque élément de G les permute. On peut donc identifier G avec un sous-groupe du groupe symétrique $\mathfrak{S}_n$.

Exercice V.D.15. Démontrer que $\mathbb{Q} \subset \mathbb{Q}\left(\sqrt[3]{2}, j\right)$ est galoisienne et que $\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt[3]{2}, j\right)/\mathbb{Q}\right)$ est isomorphe à $\mathfrak{S}_3$. En déduire que $\mathbb{Q}\left(\sqrt[3]{2}, j\right) = \mathbb{Q}\left(\sqrt[3]{2} + j\right)$ et calculer le polynôme minimal de $\sqrt[3]{2} + j$.

Exercice V.D.16. Démontrer que $\mathbb{Q} \subset \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ est galoisienne. Trouver un élément primitif α et calculer son polynôme minimal P. Est-ce que le groupe de Galois est isomorphe à $\mathfrak{S}_{\deg(P)}$?

Proposition V.D.17. Soit $\mathbb{K} \subset \mathbb{L}$ une extension finie normale et $P \in \mathbb{K}[X]$ un polynôme (de degré ≥ 1) séparable et scindé dans $\mathbb{L}$. L'action de $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ est transitive sur l'ensemble des racines de P dans $\mathbb{L}$ si et seulement si P est irréductible dans $\mathbb{K}[X]$.

Démonstration. Supposons d'abord que $P = QR$ est réductible dans $\mathbb{K}[X]$, avec $\deg(Q) \geq 1$ et $\deg(R) \geq 1$. Comme P est séparable, les racines de Q et les racines de R sont disjointes. Or, un élément du groupe de Galois envoie une racine de Q sur une racine de Q, et une racine de R sur une racine de R. L'action ne peut donc pas être transitive.

Supposons au contraire que P est irréductible dans $\mathbb{K}[X]$. Soient $\alpha, \beta \in \mathbb{L}$ des racines de P ; on cherche un élément $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ tel que $\sigma(\alpha) = \beta$. Chacun des corps $\mathbb{K}(\alpha), \mathbb{K}(\beta) \subset \mathbb{L}$ sont des corps de rupture de P. Par unicité du corps de rupture, il existe donc un $\mathbb{K}$-isomorphisme $\tau : \mathbb{K}(\alpha) \to \mathbb{K}(\beta)$ tel que $\tau(\alpha) = \beta$.

Comme $\mathbb{K} \subset \mathbb{L}$ est finie et normale, il existe un polynôme $F \in \mathbb{K}[X]$ tel que $\mathbb{L} = \mathcal{D}_{\mathbb{K}}(F)$ (**Théorème V.A.3**). Les extensions $\mathbb{K}(\alpha) \to \mathbb{L}$ et $\mathbb{K}(\alpha) \xrightarrow{\tau} \mathbb{K}(\beta) \to \mathbb{L}$ sont donc deux corps de décomposition de F sur $\mathbb{K}(\alpha)$. Encore par unicité, il existe donc un $\mathbb{K}(\alpha)$-isomorphisme $\sigma : \mathbb{L} \to \mathbb{L}$, c'est-à-dire qu'il vérifie $\sigma|_{\mathbb{K}(\alpha)} = \sigma|_{\mathbb{K}(\beta)} \circ \tau$. C'est en particulier un $\mathbb{K}$-isomorphisme (car τ en est un), c'est-à-dire un élément du groupe de Galois, et il envoie α sur β comme escompté. ◇

§ V.D(c) Théorème principal

Nous arrivons maintenant au résultat principal de cette section. Si $\mathbb{K} \subset \mathbb{L}$ est une extension finie galoisienne, alors d'après le **Théorème V.C.7** elle n'admet qu'un nombre fini d'extensions intermédiaires. La correspondance de Galois donne un moyen concret de trouver toutes ces extensions. Avant de l'énoncer, commençons par une définition :

Définition V.D.18. Soit $\mathbb{K} \subset \mathbb{L}$ une extension et $H \leq \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ un sous-groupe du groupe de Galois de l'extension. Le *corps fixe* de H est la sous-$\mathbb{K}$-extension[15] de $\mathbb{L}$ définie par :

$$\mathbb{L}^H \coloneqq \{ x \in \mathbb{L} \mid \forall \sigma \in H,\ \sigma(x) = x \}.$$

On rappelle également que si $\mathbb{K} \subset \mathbb{L}$ est galoisienne et si $\mathbb{M}$ est une sous-extension, alors $\mathbb{L} \subset \mathbb{M}$ est aussi galoisienne et $\mathrm{Gal}(\mathbb{L}/\mathbb{M})$ est un sous-groupe de $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$.

Théorème V.D.19 (Correspondance de Galois). Soit $\mathbb{K} \subset \mathbb{L}$ une extension finie galoisienne et soit $G = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ son corps de Galois. Il existe des bijections inverses l'une de l'autre, qui renversent les inclusions :

$$\begin{gathered} \Phi\colon \{\text{sous-groupes de } G\} \leftrightarrows \{\text{sous-extensions de L}\}\colon \Psi \\ H \mapsto \mathbb{L}^H \\ \mathrm{Gal}(\mathbb{L}/\mathbb{M}) \hookleftarrow \mathbb{M}. \end{gathered}$$

De plus, si $H \leq G$ est un sous-groupe, alors la sous-extension $\mathbb{L}^H$ est galoisienne si et seulement si $H \trianglelefteq G$ est distingué. Dans ce cas, on a un isomorphisme canonique $\mathrm{Gal}(\mathbb{L}^H/\mathbb{K}) = G/H$.

Remarque V.D.20. On peut « déballer » un peu l'énoncé pour le clarifier :

- Le fait que Φ et Ψ sont inverses l'une de l'autre signifie que pour toute sous-$\mathbb{K}$-extension $\mathbb{M}$, on a :
$$\mathbb{M} = \mathbb{L}^{\mathrm{Gal}(\mathbb{L}/\mathbb{M})} = \{ x \in \mathbb{L} \mid \forall \sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{M}),\ \sigma(x) = x \}.$$
Et pour tout sous-groupe $H \leq G$, on a :
$$H = \mathrm{Gal}(\mathbb{L}/\mathbb{L}^H) = \{ \sigma \in G \mid \sigma|_{\mathbb{L}^H} = \mathrm{id} \}.$$
- Le renversement des inclusions signifie que si l'on a deux sous-extensions $\mathbb{M} \subset \mathbb{M}'$ alors $\mathrm{Gal}(\mathbb{L}/\mathbb{M}')$ est un sous-groupe de $\mathrm{Gal}(\mathbb{L}/\mathbb{M})$; et si l'on a deux sous-groupes $H \leq H'$ alors $\mathbb{L}^{H'}$ est une sous-extension de $\mathbb{L}^H$.

Corollaire V.D.21. Si $\mathbb{K} \subset \mathbb{L}$ est galoisienne de groupe de Galois G, alors $\mathbb{K} = \mathbb{L}^G$.

Démonstration du théorème. On prend $\mathbb{K} \subset \mathbb{L}$ et G comme dans l'énoncé, $\mathbb{M} \subset \mathbb{L}$ une sous-extension (qui est donc finie et galoisienne) et $H \leq G$ un sous-groupe. Il est immédiat que l'on a les inclusions suivantes :

$$\mathbb{M} \subset \mathbb{L}^{\mathrm{Gal}(\mathbb{L}/\mathbb{M})}, \qquad H \subset \mathrm{Gal}(\mathbb{L}/\mathbb{L}^H).$$

Il s'agit donc de démontrer les inclusions réciproques.

Commençons par la première. Soit $\alpha \in \mathbb{L}^{\mathrm{Gal}(\mathbb{L}/\mathbb{M})}$ un élément stable sous l'action de $\mathrm{Gal}(\mathbb{L}/\mathbb{M})$ et soit $P = \mathrm{Irr}_{\mathbb{M}}(\alpha) \in \mathbb{M}[X]$ son polynôme minimal. Comme l'extension est galoisienne, P est scindé à racines simples dans $\mathbb{L}$. De plus, si $\beta \in \mathbb{L}$ est une autre racine, il existe un élément $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{M})$ tel que $\beta = \sigma(\alpha)$ d'après la **Proposition V.D.17**. Or, α est stable sous l'action du groupe de Galois, donc $\beta = \alpha$. On en déduit que P n'a qu'une seule racine. Comme il est séparable, $\deg(P) = 1$ et $\alpha \in \mathbb{M}$.

La seconde inclusion est une conséquence directe du lemme d'Artin :

Théorème V.D.22 (Lemme d'Artin). Soit $\mathbb{L}$ un corps et $H \leq \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ un groupe *fini* d'automorphismes de $\mathbb{L}$. L'extension $\mathbb{L}^H \subset \mathbb{L}$ est finie et galoisienne, de groupe de Galois H.

[15] Exercice : vérifier que c'est effectivement une sous-$\mathbb{K}$-extension.

Notons $\mathbb{M} = \mathbb{L}^H$ et soit $\alpha \in \mathbb{L}$ quelconque. On note $H \cdot \alpha \subset \mathbb{L}$ l'orbite de α sous l'action de H, qui est un ensemble fini. Posons

$$P \coloneqq \prod_{\beta \in H\cdot\alpha} (X - \beta) \in \mathbb{L}[X]$$

Ce polynôme est séparable et s'annule en α. De plus, quel que soit $\sigma \in H$, le polynôme $\sigma \cdot P$ est égal à P, donc P est à coefficients dans $\mathbb{M}$. On en déduit que $[\mathbb{M}(\alpha)\colon \mathbb{M}] \leq \deg(P) \leq |H|$ et que α est séparable sur $\mathbb{M}$.

On choisit $\gamma \in \mathbb{L}$ de degré maximal ($\leq |H|$) sur $\mathbb{M}$; démontrons que $\mathbb{L} = \mathbb{M}(\gamma)$. Étant donné $\alpha \in \mathbb{L}$ quelconque, l'extension $\mathbb{M}(\alpha, \gamma)$ est monogène d'après le théorème de l'élément primitif, disons $\mathbb{M}(\alpha, \gamma) = \mathbb{M}(z)$. Or $\mathbb{M}(\alpha, \gamma)$ est contenu dans $\mathbb{M}(\gamma)$ et γ est de degré maximal, donc $\mathbb{M}(z) = \mathbb{M}(\gamma)$ et donc finalement $\alpha \in \mathbb{M}(\alpha, \gamma) = \mathbb{M}(\gamma)$.

On conclut donc que $\mathbb{L} = \mathbb{M}(\gamma)$ est séparable et finie, de degré $\deg(\gamma) \leq |H|$. Elle est de plus normale car c'est le corps de décomposition de γ. De plus, H est un sous-groupe du groupe de Galois de $\mathbb{M} = \mathbb{L}^H \subset \mathbb{L}$. On en déduit par le **Théorème V.D.7** que l'on a les inégalités suivantes :

$$|H| \leq |\mathrm{Gal}(\mathbb{L}/\mathbb{M})| \leq [\mathbb{L}\colon \mathbb{M}]_s \leq [\mathbb{L}\colon \mathbb{M}] \leq |H|.$$

Cela permet donc bien de conclure que $H = \mathrm{Gal}(\mathbb{L}/\mathbb{M})$. ◇

Exercice V.D.23. Si $H \leq \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ est infini, démontrer que $[\mathbb{L}\colon \mathbb{K}] = \infty$.

Reprenons la démonstration du théorème principal. Le fait que Φ et Ψ renversent les inégalités est clair. Il ne nous reste donc plus qu'à démontrer le dernier point du théorème, à savoir que $H \leq G$ est distingué si et seulement si $\mathbb{K} \subset \mathbb{L}^H$ est galoisienne, et que dans ce cas, le groupe de Galois de l'extension est le quotient G/H. Cela découle du lemme suivant, dont la démonstration est claire :

Lemme V.D.24. Soit $H \leq G$ un sous-groupe du groupe de Galois et $\sigma \in G$ un élément quelconque. La sous-extension $\sigma(\mathbb{L}^H) \subset \mathbb{L}$ correspond au sous-groupe $\sigma H \sigma^{-1} \leq G$.

Commençons par supposer que $H \trianglelefteq G$ est distingué. La sous-extension $\sigma(\mathbb{L}^H)$ correspond alors à H lui-même, donc par correspondance de Galois, $\sigma(\mathbb{L}^H) = \mathbb{L}^H$. On obtient donc un morphisme de groupes :

$$\varphi\colon G \to \mathrm{Gal}(\mathbb{L}^H/\mathbb{K}).$$

Son noyau est :

$$\ker(\varphi) = \{\, \sigma \in G \mid \sigma|_{\mathbb{L}^H} = \mathrm{id} \,\} = H.$$

On obtient ainsi un morphisme injectif $G/H \to \mathrm{Gal}(\mathbb{L}^H/\mathbb{K})$. On en déduit que :

$$|\mathrm{Gal}(\mathbb{L}^H/\mathbb{K})| \geq |G/H| = |G|/|H| = [\mathbb{L}\colon \mathbb{K}]/[\mathbb{L}\colon \mathbb{L}^H] = [\mathbb{L}^H\colon \mathbb{K}].$$

Par le **Théorème V.D.7** on en déduit que $|\mathrm{Gal}(\mathbb{L}^H/\mathbb{K})| = [\mathbb{L}^H\colon \mathbb{K}]$, et donc que $\mathbb{K} \subset \mathbb{L}^H$ est galoisienne ; et que $G/H \to \mathrm{Gal}(\mathbb{L}^H/\mathbb{K})$ est un isomorphisme.

Réciproquement, supposons que $\mathbb{K} \subset \mathbb{L}^H$ est galoisienne. On considère le normalisateur de H :

$$N_G(H) \coloneqq \{\, \sigma \in G \mid \sigma H \sigma^{-1} = H \,\}.$$

D'après le raisonnement précédent, on a un morphisme $\pi\colon N_G(H) \to \mathrm{Gal}(\mathbb{L}^H/\mathbb{K})$ et son noyau est :

$$\ker(\pi) = \{\, \sigma \in N_G(H) \mid \sigma|_{\mathbb{L}^H} = \mathrm{id} \,\} = H.$$

Comme $\mathbb{K} \subset \mathbb{L}$ est normale, tout élément $\tau \in H$, c'est-à-dire tout $\mathbb{K}$-automorphisme $\tau\colon \mathbb{L}^H \to \mathbb{L}^H$, se prolonge en un $\mathbb{K}$-automorphisme $\sigma\colon \mathbb{L} \to \mathbb{L}$ (**Corollaire V.A.8**) qui vérifie $\sigma(\mathbb{L}^H) = \tau(\mathbb{L}^H) = \mathbb{L}^H$. Cette égalité entraîne que σ est un élément de $N_G(H)$, et il vérifie $\pi(\sigma) = \tau$. En d'autres termes, on a démontré que π est surjectif. On a donc :

$$|N_G(H)|/|H| = |\mathrm{Gal}(\mathbb{L}^H/\mathbb{K})| = [\mathbb{L}^H\colon \mathbb{K}] = [\mathbb{L}\colon \mathbb{K}]/[\mathbb{L}\colon \mathbb{L}^H] = |G|/|H|.$$

Donc finalement $H = N_G(H)$, c'est-à-dire que H est distingué. ◇

Section V.E. Exemples

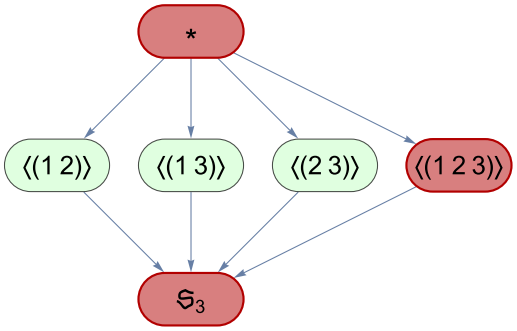
Dans cette section, nous allons donner quelques exemples de calculs de groupes de Galois.

Exemple V.E.1. Soit $\mathbb{K}$ un corps et $x \in \mathbb{K}$ un élément qui n'est pas un carré. L'extension $\mathbb{K} \subset \mathbb{L} = \mathbb{K}(\alpha)$, avec $\alpha^2 = x$ est galoisienne : c'est le corps de décomposition de $X^2 - x$, qui est irréductible. Elle est de degré 2, donc son groupe de Galois est de cardinal 2 : c'est donc le groupe cyclique $\mathfrak{S}_2 = \mathbb{Z}/2\mathbb{Z}$, dont l'unique élément non-trivial est la « conjugaison » $\sigma\colon \mathbb{K}(\alpha) \to \mathbb{K}(\alpha)$ vérifiant $\sigma(\alpha) = -\alpha$. Comme $\mathfrak{S}_2$ n'admet pas de sous-groupe non-trivial, l'extension $\mathbb{L}$ n'admet pas de sous-extension non triviale.

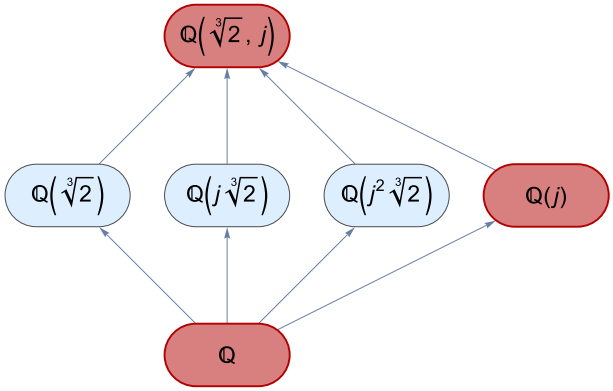
Exemple V.E.2. On a vu dans l'**Exercice V.D.15** que l'extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}, j) = \mathbb{L}$, qui est de degré 6, est galoisienne et que son groupe de Galois $G = \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ est le groupe symétrique $\mathfrak{S}_3$. Le corps $\mathbb{L}$ est le corps de décomposition de $X^3 - 2$, dont les racines sont $x_1 = j\sqrt[3]{2}$, $x_2 = j^2\sqrt[3]{2}$ et $x_3 = j^3\sqrt[3]{2} = \sqrt[3]{2}$. Le groupe de Galois agit par permutation des racines. Il est engendré par les deux permutations $\sigma = (1,2)$ (une transposition) et $\tau = (1,2,3)$ (un cycle d'ordre 3), qui agissent ainsi sur les racines :

- La transposition $\sigma = (1\ \ 2)$ échange x_1 et $x_2 = \bar{x}_1$ et fixe x_3. Il s'agit donc de la conjugaison complexe : $\sigma(z) = \bar{z}$ pour tout $z \in \overline{\mathbb{L}}$. Son sous-corps fixe est $\mathbb{Q}(\sqrt[3]{2})$.
- Le cycle $\tau = (1\ \ 2\ \ 3)$ permute les racines de façon cyclique, par $\tau(x_1) = x_2 = jx_1$, $\tau(x_2) = x_3 = jx_1$ et $\tau(x_3) = x_1 = jx_3$. Attention, on n'a pas $\tau(z) = jz$ pour tout z ; par exemple, $\tau(1) = 1 \neq j$. Son sous-corps fixe est $\mathbb{Q}(j)$.

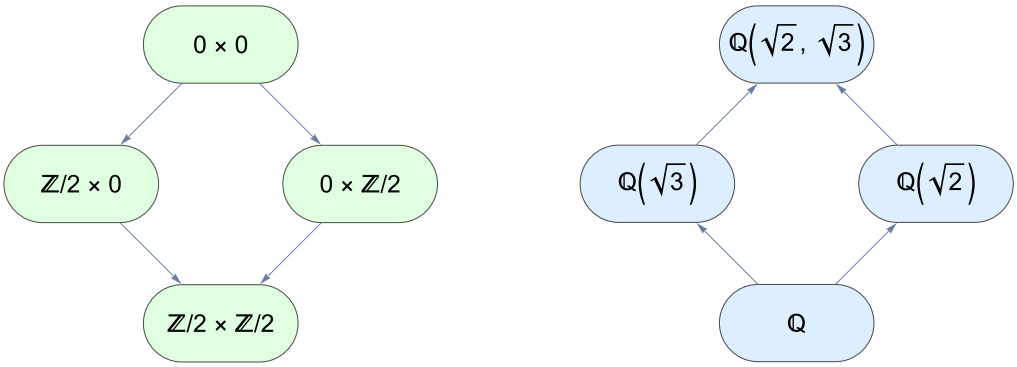
Le seul sous-groupe distingué non-trivial de G est le groupe alterné $\mathfrak{A}_3 = \langle (1\ \ 2\ \ 3) \rangle$, qui est d'ordre 3. On peut lister tous les sous-groupes de G et leurs inclusions de la façon suivante, avec en rouge les sous-groupes distingués :



Ces sous-groupes correspondent aux sous-extensions de $\mathbb{Q}(\sqrt[3]{3}, j)$. Le groupe alterné correspond à la seule sous-extension galoisienne non-triviale $\mathbb{Q}(j)$, qui est quadratique : $[\mathfrak{S}_3\colon \mathfrak{A}_3] = 2$. Nous pouvons lister toutes les sous-extensions, avec en rouge les extensions galoisiennes :



Exercice V.E.3. L'extension $\mathbb{Q} \subset \mathbb{L} = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ est galoisienne : c'est le corps de décomposition de $(X^2-2)(X^2-3)$, dont les racines sont $x_1 = \sqrt{2}$, $x_2 = -\sqrt{2}$, $x_3 = \sqrt{3}$ et $x_4 = -\sqrt{3}$. Elle est de degré 4, avec une base donnée par $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$. Son groupe de Galois, qui est un sous-groupe de $\mathfrak{S}_4$, est donc de cardinal 4. Il est engendré par les deux transpositions $\sigma = (1\ \ 2)$ et $\tau = (3\ \ 4)$, donc il est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, qui est abélien. Ses quatre sous-groupes sont donc distingués et les quatre sous-extensions correspondantes sont galoisiennes :



Exemple V.E.4. Soit $P = X^5 - 6X + 3 \in \mathbb{Q}[X]$. Ce polynôme est irréductible (critère d'Eisenstein). Une étude de fonction montre qu'il a trois racines réelles distinctes $x_1, x_2, x_3 \in \mathbb{R}$ et donc deux racines complexes conjuguées $x_4 = \bar{x}_5 \in \mathbb{C} \setminus \mathbb{R}$ distinctes. Soit $\mathbb{L} = \mathcal{D}_{\mathbb{Q}}(P) \subset \mathbb{C}$ son corps de décomposition. C'est une extension galoisienne de $\mathbb{Q}$.

Son groupe de Galois $G = \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ est un sous-groupe du groupe symétrique $\mathfrak{S}_5$. La transposition $\sigma = (4\ \ 5)$ appartient à G : c'est la conjugaison complexe. De plus, $\mathbb{L}$ contient la sous-extension $\mathbb{Q}(x_1)$, qui est de degré 5. Le cardinal de G est donc divisible par 5, donc d'après le théorème de Cauchy, il contient un élément $\tau \in G$ d'ordre 5. Les éléments d'ordre de 5 dans $\mathfrak{S}_5$ sont les 5-cycles. Quitte à remplacer τ par une de ses puissances, on peut supposer que $\tau(4) = 5$; quitte à renuméroter x_1, x_2, x_3, on peut supposer que $\tau = (1\ \ 2\ \ 3\ \ 4\ \ 5)$. La famille (σ, τ) engendre $\mathfrak{S}_5$, donc $G = \mathfrak{S}_5$.

Notons que $\mathfrak{S}_5$ contient un seul sous-groupe distingué, le groupe alterné $\mathfrak{A}_5$ (d'indice 2). L'extension $\mathbb{L}$ ne contient donc qu'une seule sous-extension galoisienne non triviale, qui est quadratique.

Exemple V.E.5. Soit $\alpha = \sqrt[4]{2}$. L'extension $\mathbb{Q} \subset \mathbb{L} = \mathbb{Q}(\alpha)$, qui est de degré 4, n'est pas galoisienne. C'est le corps de rupture de $P = X^4 - 2$. Ce polynôme est irréductible et admet une racine dans $\mathbb{L}$. Mais P n'est pas scindé sur $\mathbb{L}$. En effet, on peut le factoriser en $(X-\alpha)(X+\alpha)(X^2+\alpha^2)$; or, $X^2 + \alpha^2$ n'admet pas de racine réelle, donc il est irréductible sur $\mathbb{Q}(\alpha) \subset \mathbb{R}$.

Un élément du groupe de Galois $G = \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ est entièrement déterminé par $\sigma(\alpha) \in \mathbb{L}$, qui doit vérifier $\sigma(\alpha)^2 = 2$. Cette équation n'a que deux solutions dans $\mathbb{L}$, à savoir α et $-\alpha$. Le groupe de Galois ne contient donc que deux éléments, l'identité (qui vérifie $\sigma(\alpha) = \alpha$) et la « conjugaison » (qui vérifie $\sigma(\alpha) = -\alpha$). On remarque que $\alpha^2 \notin \mathbb{Q}$ est stable par l'action de G, car $\sigma(\alpha^2) = (-\alpha)^2 = \alpha^2$. En fait, le corps fixe $\mathbb{L}^G$ est égal à $\mathbb{Q}(\alpha^2) \subsetneq \mathbb{L}$. Cette sous-extension de $\mathbb{L}$ ne correspond à aucun des deux sous-groupes de $G \cong \mathbb{Z}/2\mathbb{Z}$.

Pour obtenir une extension galoisienne de $\mathbb{Q}$, on construit le corps de décomposition de $X^4 - 2$ en rajoutant la racine « manquante » de $X^2 + \alpha^2 = (X - i\alpha)(X + i\alpha)$; on considère $\mathbb{M} = \mathbb{L}(i) = \mathbb{Q}(i, \alpha)$. Dans ce corps, les quatre racines de P sont α, $-\alpha$, $i\alpha$ et $-i\alpha$, et $\mathbb{M}$ est son corps de décomposition. L'extension $\mathbb{M}$ est de degré 8 sur $\mathbb{Q}$ et un élément primitif est donné par $i + \sqrt[4]{2}$ (racine de $1 + 28x^2 + 2x^4 + 4x^6 + x^8$).

Comme l'extension $\mathbb{Q} \subset \mathbb{M}$ est galoisienne, $G = \mathrm{Gal}(\mathbb{M}/\mathbb{Q})$ est d'ordre $[\mathbb{M}:\mathbb{Q}] = 8$. Il existe cinq groupes d'ordre 8 à isomorphisme près : $(\mathbb{Z}/2\mathbb{Z})^3$, $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$, $\mathbb{Z}/8\mathbb{Z}$, le groupe diédral D_8 et le groupe des quaternions unitaires Q_8. Nous allons déterminer auquel de ces groupes G est isomorphe.

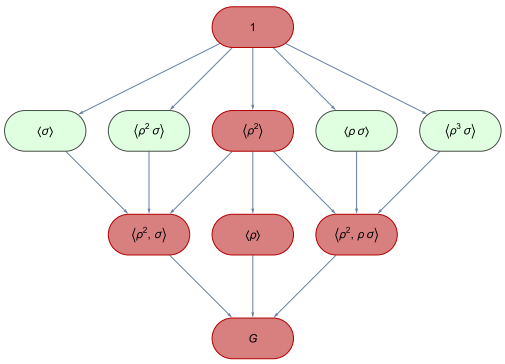
La conjugaison complexe $\sigma : \mathbb{M} \to \mathbb{M}$ donne un premier automorphisme de $\mathbb{M}$, qui vérifie $\sigma^2 = 1$.

Par multiplicativité du degré, $8 = [\mathbb{M}:\mathbb{Q}] = [\mathbb{M}:\mathbb{L}] \cdot [\mathbb{L}:\mathbb{Q}] = [\mathbb{M}:\mathbb{Q}(i)] \cdot [\mathbb{Q}(i):\mathbb{Q}]$, d'où $[\mathbb{M}:\mathbb{L}] = 2$ et $[\mathbb{M}:\mathbb{Q}(i)] = 4$. On en déduit que $P = X^4 - 2$ est irréductible sur $\mathbb{Q}(i)$. En effet, s'il ne l'était pas, on aurait $P = QR$ avec $\deg(Q) + \deg(R) = 4$, $\deg(Q), \deg(R) \geq 1$, ce qui entraînerait :

- Si les deux polynômes Q et R étaient de degré 2, alors $\mathbb{M} = \mathbb{Q}(i)(\alpha)$ serait le corps de rupture de Q ou R et serait donc de degré 2 sur $\mathbb{Q}(i)$, une contradiction ;
- Si Q ou R était de degré 1, cela signifierait que P admet une racine dans $\mathbb{Q}(i)$ et que $\mathbb{Q}(i)$ contiendrait donc une copie du corps de rupture de P ; or, ce corps de rupture est isomorphe à $\mathbb{Q}(\alpha)$ qui est de degré 4 sur $\mathbb{Q}$, donc on aurait $[\mathbb{Q}(i):\mathbb{Q}] \geq 4$, une contradiction.

Comme $\mathbb{Q} \subset \mathbb{M}$ est normale, $\mathbb{L} \subset \mathbb{M}$ l'est aussi. Donc $\mathrm{Gal}(\mathbb{M}/\mathbb{L})$ agit transitivement sur les racines du polynôme irréductible P. Il existe donc un automorphisme $\rho : \mathbb{M} \to \mathbb{M}$ tel que $\rho(\alpha) = i\alpha$; et comme $\rho|_{\mathbb{L}} = 1$, on a $\rho(i) = i$. On calcule que $\rho^2(\alpha) = i^2\alpha = -\alpha \neq \alpha$, $\rho^3(\alpha) = i^3\alpha = -i\alpha \neq \alpha$, et $\rho^4 = \mathrm{id}$, donc ρ est d'ordre 4 et $\langle\rho\rangle$ est d'index 2.

De plus, $\rho \notin \langle\sigma\rangle$ donc G est engendré par la famille (σ, ρ). Enfin, on peut vérifier que $\sigma\rho\sigma^{-1} = \rho^3$ facilement sur les deux générateurs. On reconnaît la présentation standard du groupe diédral D_8 auquel G est donc isomorphe. Les sous-groupes de G s'organisent ainsi, avec en rouge les sous-groupes distingués :



Exercice V.E.6. Déterminer les sous-extensions qui correspondent à chacun de ces sous-groupes.

Chapitre VI. GROUPES ABÉLIENS DE TYPE FINI

> « Démontrer que deux nombres a et b sont égaux en démontrant d'abord que $a \leq b$ puis que $a \geq b$ est injuste ; il faut plutôt démontrer qu'ils sont vraiment égaux en dévoilant la raison profonde de leur égalité. »
>
> Emmy Noether (citée par Hermann Weyl)

Dans ce dernier chapitre, nous allons donner quelques outils pour l'algèbre linéaire « sur les entiers » (ou plus généralement les anneaux euclidiens), ainsi qu'une application remarquable : le théorème de structure des groupes abéliens de type fini.

Section VI.A. Bases du calcul matriciel sur $\mathbb{Z}$

Commençons par quelques rappels élémentaires.

Notation VI.A.1. Soit i, j des entiers. On note $\delta_{i,j}$ le *delta de Kronecker*, défini par :

$$\delta_{i,j} \coloneqq \begin{cases} 1, & \text{si } i = j; \\ 0, & \text{sinon.} \end{cases}$$

Notation VI.A.2. Soit A un anneau et $p, q \geq 1$ deux entiers. On note $\mathcal{M}_{p,q}(A) = (A^q)^p$ l'ensemble des *matrices* à p lignes et q colonnes à coefficients dans A. Si $p = q$, on note $\mathcal{M}_p(A) = \mathcal{M}_{p,p}(A)$ l'ensemble des matrices *carrées*. Si M est un élément de $\mathcal{M}_{p,q}(A)$ et $1 \leq i \leq p$, $1 \leq j \leq q$ sont des entiers, on note $M_{i,j} \in A$ le coefficient de M à l'intersection de la $i$ème ligne et de la $j$ème colonne.

On note $0 \in \mathcal{M}_{p,q}(A)$ la *matrice nulle* définie par $0_{i,j} = 0 \in A$. Pour $p = q$, on note $I_p \in \mathcal{M}_p(A)$ la *matrice identité*, définie par :

$$\left(I_p\right)_{i,j} \coloneqq \delta_{i,j}.$$

C'est un exemple de *matrice diagonale*, c'est-à-dire une matrice carrée $M \in \mathcal{M}_p(A)$ telle que, pour $1 \leq i \neq j \leq p$, on a $M_{i,j} = 0$.

Étant donnée $M \in \mathcal{M}_{p,q}(A)$, on note ${}^tM \in \mathcal{M}_{q,p}(A)$ sa transposée, définie par $M_{j,i} \coloneqq {}^tM_{i,j}$.

Proposition VI.A.3. Quels que soient p, q, le triplet $\left(\mathcal{M}_{p,q}(A), +, 0\right)$ forme un groupe abélien. La multiplication matricielle $\mathcal{M}_{p,q}(A) \times \mathcal{M}_{q,r}(A) \to \mathcal{M}_{p,r}(A)$ est associative et distributive par rapport à la multiplication, et les matrices identité sont des éléments neutres pour la multiplication. Ces structures font de $\left(\mathcal{M}_p(A), \times, I_p\right)$ un anneau.

Remarque VI.A.4. Si $p = 0$ ou $q = 0$ on note parfois $\mathcal{M}_{p,q}(A) = 0$, le groupe abélien trivial.

Remarque VI.A.5. L'anneau $\mathcal{M}_1(A)$ est bien sûr isomorphe à A.

Définition VI.A.6. Soit $M \in \mathcal{M}_p(A)$ une matrice carrée. Son *déterminant* est l'élément $\det(M) \in A$ défini par la formule suivante, où $\varepsilon(\sigma)$ désigne la signature d'une permutation :

$$\det(M) \coloneqq \sum_{\sigma \in \mathfrak{S}_n} \prod_{i=1}^{p} \varepsilon(\sigma) M_{i,\sigma(i)}.$$

Proposition VI.A.7. Le déterminant est multiplicatif : pour tout $M, N \in \mathcal{M}_p(A)$, on a $\det(MN) = \det(M) \cdot \det(N)$. On peut calculer le déterminant en développant selon une ligne ou une colonne. La matrice nulle a pour déterminant 0, la matrice identité a pour déterminant 1.

Définition VI.A.8. Soit $M \in \mathcal{M}_p(A)$ une matrice carrée avec $p \geq 2$. Sa *comatrice* est la matrice $\mathrm{com}(M) \in \mathcal{M}_p(A)$ définie par $\mathrm{com}(M)_{i,j} = (-1)^{i+j}\delta_{i,j}(M)$, où $\delta_{i,j}(M)$ est le déterminant du mineur de M obtenu en retirant la $i$ème ligne et la $j$ème colonne.

Exemple VI.A.9. Soit $M \in \mathcal{M}_2(A)$ une matrice carrée de taille 2 donnée par :

$$M = \begin{pmatrix} m_{1,1} & m_{1,2} \\ m_{2,1} & m_{2,2} \end{pmatrix}.$$

Alors sa comatrice est égale à :

$$\mathrm{com}(M) = \begin{pmatrix} m_{2,2} & -m_{2,1} \\ -m_{1,2} & m_{1,1} \end{pmatrix}.$$

Proposition VI.A.10. Quel que soit $M \in \mathcal{M}_p(A)$, on a $M \cdot {}^t\mathrm{com}(M) = \det(M) \cdot I_p = {}^t\mathrm{com}(M) \cdot M$.

Lemme VI.A.11. Une matrice carrée M est inversible si et seulement si $\det(M) \in A^\times$. Dans ce cas, son inverse est la matrice :

$$M^{-1} = (\det(M))^{-1} \cdot {}^t\mathrm{com}(M).$$

Une telle matrice est appelée une *matrice unimodulaire* (pour les distinguer des matrices qui seraient inversibles dans le corps des fractions de A).

Lemme VI.A.12. Une matrice entière est inversible si et seulement si son déterminant est ± 1.

Remarque VI.A.13. La plupart du temps, on emploie le terme « unimodulaire » pour les matrices à coefficients dans $\mathbb{Z}$, donc pour les matrices de déterminant ± 1.

Définition VI.A.14. On note $\mathrm{GL}_p(A)$ l'ensemble des matrices carrées de taille p inversibles à coefficients dans A. Cet ensemble forme un groupe pour la multiplication.

Section VI.B. Opérations élémentaires

Définition VI.B.1. Soit $M \in \mathcal{M}_{p,q}(A)$ une matrice. Une *opération élémentaire sur les lignes* de M est l'une des trois opérations suivantes, qui produit une nouvelle matrice M' :

a) La permutation de deux lignes i et j, notée $L_i \leftrightarrow L_j$, produit une matrice M' telle que :
$$M'_{k,l} = \begin{cases} M_{k,l}, & \text{si } k \notin \{i, j\}; \\ M_{j,l}, & \text{si } k = i; \\ M_{i,l}, & \text{si } k = j. \end{cases}$$

b) La multiplication d'une ligne i par un facteur inversible $\lambda \in A^\times$, notée $L_i \leftarrow \lambda L_i$, produit une matrice M' telle que :
$$M'_{k,l} = \begin{cases} \lambda M_{i,l}, & \text{si } k = i \\ M_{k,l}, & \text{sinon.} \end{cases}$$

c) L'ajout à une ligne i d'un multiple (par $a \in A$) d'une autre ligne j, noté $L_i \leftarrow L_i + aL_j$, produit une matrice M' telle que :
$$M'_{k,l} = \begin{cases} M_{i,l} + aM_{j,l}, & \text{si } k = i \\ M_{k,l}, & \text{sinon.} \end{cases}$$

Les *opérations élémentaires* sur les colonnes sont définies de façon analogue.

Dans la proposition suivante, on notera $E_{i,j} \in \mathcal{M}_{p,q}(A)$ la matrice qui ne contient qu'une seule entrée non nulle en position (i,j) qui vaut 1, c'est-à-dire :

$$\left(E_{i,j}\right)_{k,l} = \delta_{i,k}\delta_{j,l}.$$

Proposition VI.B.2. Les trois types d'opérations élémentaires sur les lignes (resp., colonnes) correspondent à la multiplication à gauche (resp., à droite) par les types de matrices suivants :

a) La permutation de deux lignes/colonnes correspond à la multiplication par la matrice de permutation (les entrées non triviales sont en lignes/colonnes i et j) :

$$\begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & \ddots & \square & \square & \square & \square & \vdots \\ \vdots & \square & 0 & \cdots & 1 & \square & \vdots \\ \vdots & \square & \vdots & \ddots & \vdots & \square & \vdots \\ \vdots & \square & 1 & \cdots & 0 & \square & \vdots \\ \vdots & \square & \square & \square & \square & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 1 \end{pmatrix} = I_p - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}.$$

b) L'ajout d'un multiple d'une ligne/colonne à une autre ligne/colonne correspond à la matrice diagonale (l'entrée non triviale est en position (i,j) ou (j,i) suivant les cas) :

$$\begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & \ddots & \square & \square & \square & \square & \vdots \\ \vdots & \square & 1 & \square & \square & \square & \vdots \\ \vdots & \square & \vdots & \ddots & \square & \square & \vdots \\ \vdots & \square & a & \cdots & 1 & \square & \vdots \\ \vdots & \square & \square & \square & \square & \ddots & 0 \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & 1 \end{pmatrix} = I_p + aE_{i,j} \quad (\text{resp., } I_p + aE_{j,i} \text{ pour les colonnes}).$$

c) La multiplication d'une ligne/colonne i par un facteur inversible $\lambda \in A^\times$ correspond à la matrice diagonale (l'entrée non triviale est en position (i,i)) :

$$\begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & \square & \square & \vdots \\ \vdots & \square & \lambda & \square & \vdots \\ \vdots & \square & \square & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix} = I_p + (\lambda - 1)E_{i,i}.$$

De plus, les trois types de matrices sont unimodulaires et leur inverse est du même type.

Définition VI.B.3. On note $\mathcal{E}_p(A)$ le sous-groupe de $\mathrm{GL}_p(A)$ engendré par les matrices du type ci-dessus.

Remarque VI.B.4. Si $P \in \mathcal{E}_p(A)$, $M \in \mathcal{M}_{p,q}(A)$ et $Q \in \mathcal{E}_q(A)$ sont trois matrices, alors PM est une matrice obtenue à partir de M en effectuant une suite d'opérations élémentaires sur les lignes, tandis que MQ est obtenue à partir de M en effectuant une suite d'opérations élémentaires sur les colonnes. La matrice PMQ est obtenue en effectuant une suite d'opérations élémentaires sur les lignes et les colonnes.

Section VI.C. Formes normales

§ VI.C(a) Équivalence de matrices

Définition VI.C.1. Soit $M, M' \in \mathcal{M}_{p,q}(A)$ deux matrices. On dit qu'elles sont *équivalentes* s'il existe deux matrices inversibles $U \in \mathrm{GL}_p(A)$ et $V \in \mathrm{GL}_q(A)$ telles que $M' = UMV$. On dit qu'elles sont *équivalentes à gauche* (resp., à *droite*) s'il existe une matrice $U \in \mathrm{GL}_p(A)$ (resp., $V \in \mathrm{GL}_q(A)$) telle que $M' = UM$ (resp., $M' = MV$).

Remarque VI.C.2. Il ne faut pas confondre cette notion avec la notion de matrices semblables (c.-à-d., des matrices carrées M et M' telles qu'il existe U inversible telle que $M' = UMU^{-1}$. En termes d'applications linéaires, deux matrices équivalentes représentent la même application linéaire en changeant de base au départ et à l'arrivée indépendamment ; alors que des matrices semblables représentent le même endomorphisme après avoir effectué le même changement de base au départ et à l'arrivée.

En règle générale, la notion précédente n'est pas équivalente à la suivante :

Définition VI.C.3. Soit $M, M' \in \mathcal{M}_{p,q}(A)$ deux matrices. On dit qu'elles sont *élémentairement équivalentes* s'il existe deux matrices $P \in \mathcal{E}_p(A)$ et $Q \in \mathcal{E}_q(A)$ telles que $M' = PMQ$. On dit qu'elles sont équivalentes à gauche (resp., à droite) s'il existe une matrice $P \in \mathcal{E}_p(A)$ (resp., $Q \in \mathcal{E}_q(A)$) telle que $M' = PM$ (resp., $M' = MQ$).

Remarque VI.C.4. Comme $\mathcal{E}_p(A) \subset \mathrm{GL}_p(A)$, si deux matrices sont élémentairement équivalentes (resp., à droite, resp., à gauche) alors elles sont équivalentes (resp., à droite, resp., à gauche).

Notre objectif, dans cette section, est de ramener toute matrice à une matrice équivalente sous forme « normale » à l'aide d'opérations élémentaires.

§ VI.C(b) Sur un corps

Définition VI.C.5. Soit $\mathbb{K}$ un corps et $M \in \mathcal{M}_{p,q}(\mathbb{K})$ une matrice. Le *rang* de M, noté $\mathrm{rg}(M)$, est la dimension du sous-espace vectoriel de $\mathbb{K}^p$ engendré par les q vecteurs colonnes de M.

Remarque VI.C.6. Ce nombre est aussi égal au rang de la transposée, c'est-à-dire la dimension du sous-espace vectoriel de $\mathbb{K}^q$ engendré par les p vecteurs ligne de M (cf. cours de licence).

Proposition VI.C.7. Si $\mathbb{K}$ est un corps, deux matrices $M, M' \in \mathcal{M}_{p,q}(\mathbb{K})$ sont équivalentes si et seulement si elles ont le même rang.

Démonstration. Le rang est préservé par les opérations élémentaires, car l'image d'un sous-espace vectoriel (ici, l'image ou la coimage de la matrice) par une application linéaire inversible garde la même dimension. Donc deux matrices équivalentes ont le même rang.

L'algorithme du pivot de Gauss donne une démonstration de la réciproque. Il permet de transformer, à l'aide d'opérations élémentaires sur les lignes, une matrice quelconque M en une matrice *échelonnée réduite*, c'est-à-dire une matrice $M' = PM$ (avec $P \in \mathcal{E}_p(\mathbb{K})$) telle que :

- Le nombre de zéros à gauche du premier coefficient non-nul d'une ligne (le « pivot ») augmente strictement ligne après ligne, jusqu'à éventuellement plafonner au nombre de colonnes ;
- Chaque pivot vaut 1 ;
- Si une colonne contient un pivot, alors tous les autres coefficients de cette colonne sont nuls.

Visuellement, il s'agit d'une matrice de cette forme (les $*$ sont des nombres quelconques) :

$$\begin{pmatrix} 1 & * & 0 & 0 & * & * & 0 \\ 0 & 0 & 1 & 0 & * & * & 0 \\ 0 & 0 & 0 & 1 & * & * & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Schématiquement, l'algorithme procède ainsi, pour $M \in \mathcal{M}_{p,q}(\mathbb{K})$:

- On commence par poser $h = 1$ et $k = 1$.
- Tant que $h \leq p$ et $k \leq q$, on effectue les étapes suivantes :
  - On note i_0 le premier indice $i \geq h$ tel que $m_{i,k} \neq 0$;
  - Si i_0 n'existe pas, on incrémente simplement k ;
  - Sinon :
    - On échange les lignes h et i_0 de M ($L_{i_0} \leftrightarrow L_h$) ;
    - On divise la ligne h par $m_{h,k}$ ($L_h \leftarrow m_{h,k}^{-1} L_h$) ;
    - Pour chaque $i \geq h + 1$, on soustrait de la ligne i la ligne h multipliée par $m_{i,k}$ ($L_i \leftarrow L_i - m_{i,k} L_h$).
- Pour chaque ligne i qui contient un élément non nul :
  - On note j la colonne qui contient le premier élément non nul de la ligne i, nécessairement un 1 à la suite de l'algorithme précédent ;
  - Pour chaque $i' < i$, on soustrait à de ligne i' la ligne i multipliée par $m_{i',j}$ ($L_{i'} \leftarrow m_{i',j} L_i$).

En code Mathematica :

```
pivot[m_] := Module[{m2, p, q, h, k, i0, j},
  m2 = m;
  {p, q} = Dimensions[m2];
  h = 1; k = 1;
  While[h <= p && k <= q,
   i0 = SelectFirst[Range[h, p], m2[[#1, k]] != 0 & ];
   If[! MissingQ[i0],
    m2[[{i0, h}]] = m2[[{h, i0}]];
    m2[[h]] = m2[[h]]/m2[[h, k]];
    m2[[h + 1 ;; All]] =
     m2[[h + 1 ;; All]] -
      m2[[h + 1 ;; All, k]] ⊗ m2[[h]];
    h++];
   k++];
  Do[
   j = SelectFirst[Range[p], m2[[i, #1]] != 0 & ];
   If[! MissingQ[j],
    m2[[1 ;; i - 1]] =
     m2[[1 ;; i - 1]] - Threaded[m2[[1 ;; i - 1, j]] ⊗ m2[[i]]]
    ],
   {i, 2, p}];
  m2
]
```

L'algorithme ne « casse » pas les pivots préexistants ni les zéro sur leur colonne. En appliquant une seconde fois l'algorithme à ${}^tM'$, c'est-à-dire en opérant sur les colonnes plutôt que les lignes, on obtient donc une matrice $M'' = M'Q = PMQ$ (avec $Q \in \mathcal{E}_q(\mathbb{K})$) qui se décompose par blocs :

$$M'' = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix},$$

Où I_r est la matrice identité de rang r et où l'on complète par des zéros les lignes et colonnes manquantes. N'importe quelles matrices de rang r peuvent donc être ramenées à cette matrice de type identité et elles sont donc toutes équivalentes. ◇

Corollaire VI.C.8. Si $\mathbb{K}$ est un corps, alors $\mathcal{E}_p(\mathbb{K}) = \mathrm{GL}_p(\mathbb{K})$.

Démonstration. On a bien $\mathcal{E}_p(\mathbb{K}) \subset \mathrm{GL}_p(\mathbb{K})$. Réciproquement, si une matrice $M \in \mathrm{GL}_p(\mathbb{K})$ est inversible, elle est de rang maximal $r = p$ et elle est donc équivalente à la matrice identité I_p. Il existe donc $P, Q \in \mathcal{E}_p(\mathbb{K})$ tels que $M = PI_pQ = PQ$ et donc $M \in \mathcal{E}_p(\mathbb{K})$. ◇

Corollaire VI.C.9. Deux matrices à coefficients dans un corps sont équivalentes si et seulement si elles sont élémentairement équivalentes.

Sur un anneau quelconque, on ne peut pas ramener toutes les matrices à des matrices de type « identité ». L'algorithme du pivot de Gauss utilise de manière cruciale la division par des éléments arbitraires de l'anneau, ce qui n'est pas possible en général.

Exemple VI.C.10. Le problème est assez clair en dimension 1 sur $A = \mathbb{Z}$. On ne peut pas transformer la matrice $M = (2) \in \mathcal{M}_1(\mathbb{Z})$ en la matrice « normale » $(1) \in \mathcal{M}_1(\mathbb{Z})$ par des opérations élémentaires.

Exercice VI.C.11. Démontrer que les deux matrices suivantes ne sont pas équivalentes sur $\mathbb{Z}$ (indication : le PGCD des coefficients d'une matrice 2×2 n'est pas modifié par les opérations élémentaires) :

$$M = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, \qquad M' = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Dans les sections suivantes, nous allons généraliser la notion de forme normale au cas des anneaux euclidiens. Plusieurs des résultats qui suivent restent vrais pour les anneaux principaux, mais la preuve est plus délicate.

§ VI.C(c) Forme normale d'Hermite

Commençons par une généralisation de la notion de « forme échelonnée » pour les matrices à coefficients dans un anneau euclidien. Pour un anneau euclidien A, on rappelle qu'on a une application $\nu : A \to \mathbb{N} \cup \{-\infty\}$ telle que $\nu^{-1}(\{-\infty\}) = \{0\}$ et pour tous $a, b \in A$, $b \neq 0$, il existe $q, r \in A$ tels que $a = bq + r$ et $\nu(r) < \nu(b)$.

Théorème VI.C.12 (Forme normale d'Hermite). Soit A un anneau euclidien et $M \in \mathcal{M}_{p,q}(A)$ une matrice de taille $p \times q$ à coefficients dans A. La matrice M est élémentairement équivalente à gauche (resp., à droite) à une matrice triangulaire supérieure (resp., inférieure) $H \in \mathcal{M}_{p,q}(A)$ de la forme :

	Équivalence à gauche	**Équivalence à droite**
$\boldsymbol{p \leq q}$	$H = \begin{pmatrix} h_{1,1} & \cdots & h_{1,p} & \cdots & h_{1,q} \\ 0 & \ddots & \vdots & * & \vdots \\ 0 & 0 & h_{p,p} & \cdots & h_{p,q} \end{pmatrix}$	$H = \begin{pmatrix} h_{1,1} & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & 0 & \vdots & 0 & \vdots \\ h_{p,1} & \cdots & h_{p,p} & 0 & \cdots & 0 \end{pmatrix}$
$\boldsymbol{p \geq q}$	$H = \begin{pmatrix} h_{1,1} & \cdots & h_{1,q} \\ 0 & \ddots & \vdots \\ 0 & 0 & h_{q,q} \\ 0 & \cdots & 0 \\ \vdots & 0 & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$	$H = \begin{pmatrix} h_{1,1} & 0 & 0 \\ \vdots & \ddots & 0 \\ h_{q,1} & \cdots & h_{q,q} \\ \vdots & * & \vdots \\ h_{p,1} & \cdots & h_{p,q} \end{pmatrix}$

De plus, les coefficients $\{h_{i,j}\}$ vérifient les conditions suivantes, pour tous $i < j$:

- Si $h_{j,j}$ (resp., $h_{i,i}$) est non nul et non inversible, alors $\nu(h_{i,j}) < \nu(h_{j,j})$ (resp., $\nu(h_{j,i}) < \nu(h_{i,i})$) ;
- Si $h_{j,j}$ (resp., $h_{i,i}$) est inversible, alors $h_{i,j} = 0$ (resp., $h_{j,i} = 0$).

Un couple (U, H) formé d'une matrice élémentaire $U \in \mathcal{E}_p(A)$ et d'une matrice H comme ci-dessus tel que $UM = H$ (resp., $MU = H$) est appelé *forme normale d'Hermite* (supérieure, resp., inférieure) de M.

Remarque VI.C.13. Si on se rappelle que $v(0) = -\infty$ et que les éléments inversibles $u \in A^\times$ d'un anneau euclidien sont caractérisés par le fait que $v(u)$ est la valeur minimale de v (c'est-à-dire $v(u) = v_0$ ne dépend pas de $u \in A^\times$ et si $a \in A \setminus \{0\}$ n'est pas inversible, alors $v(a) > v_0$), on peut condenser la définition : « si $h_{j,j} \neq 0$, alors pour $i < j$, $v(h_{i,j}) < v(h_{j,j})$ » (et l'analogue pour la forme normale inférieure).

Remarque VI.C.14. Si A est un corps, on retrouve la définition d'une matrice sous forme échelonnée.

Exemple VI.C.15. Soit $M = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 2 \\ 6 & 7 & 9 \end{pmatrix} \in \mathcal{M}_3(\mathbb{Z})$. Une forme normale d'Hermite supérieure de M est donnée par le couple :

$$U = \begin{pmatrix} -1 & -1 & 1 \\ 2 & -2 & 1 \\ 2 & -5 & 3 \end{pmatrix} \in \mathcal{E}_2(\mathbb{Z}), \qquad H = \begin{pmatrix} 1 & 0 & 4 \\ 0 & 1 & 11 \\ 0 & 0 & 23 \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}).$$

Une forme normale d'Hermite inférieure est :

$$U = \begin{pmatrix} 2 & 8 & 11 \\ -2 & -7 & -10 \\ 1 & 2 & 3 \end{pmatrix} \in \mathcal{E}_2(\mathbb{Z}), \qquad H = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 7 & 17 & 23 \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}).$$

Démonstration du théorème. Nous allons démontrer le théorème pour les formes normales supérieures ; l'existence des formes normales inférieures en découle immédiatement en passant aux transposées. Nous allons procéder par récurrence sur le nombre q de colonnes de la matrice. Le lemme suivant donne le cas $q = 1$:

Lemme VI.C.16. Soit $X \in \mathcal{M}_{p,1}(A)$ un vecteur colonne (resp., $X \in \mathcal{M}_{1,p}(A)$ un vecteur ligne) dont les coefficients sont $x_1, \dots, x_p$. Soit $d = x_1 \wedge \dots \wedge x_p$ le PGCD des coefficients de X. Le vecteur X est équivalent à gauche (resp., à droite) au vecteur dont les coefficients sont $d, 0, \dots, 0$.

Démonstration. Il suffit d'appliquer l'algorithme d'Euclide étendu pour obtenir le résultat. On vérifiera que les opérations qui interviennent dans cet algorithme se traduisent en opérations élémentaires sur les lignes de C. ◇

Exemple VI.C.17. Supposons que $X = (6 \quad 15 \quad 10) \in \mathcal{M}_{1,3}(\mathbb{Z})$. Le PGCD des entrées de X vaut $1 = 6x_1 - 3x_2 + x_3$. Pour savoir quelles opérations élémentaires appliquer, il faut suivre pas à pas l'algorithme d'Euclide étendu :

Avant	Division euclidienne	Opération	Après
On commence par calculer le PGCD de $x_1 = 6$ et $x_2 = 15$			
$(6 \quad 15 \quad 10)$	$15 = 2 \cdot 6 + 3$	$C_2 \leftarrow C_2 - 2C_1$	$(6 \quad 3 \quad 10)$
$(6 \quad 3 \quad 10)$	$6 = 2 \cdot 3 + 0$	$C_1 \leftarrow C_1 - 2C_2$	$(0 \quad 3 \quad 10)$
On calcule le PGCD de $x_2 = 3$ et $x_3 = 10$			
$(0 \quad 3 \quad 10)$	$10 = 3 \cdot 3 + 1$	$C_3 \leftarrow C_3 - 3C_2$	$(0 \quad 3 \quad 1)$
$(0 \quad 3 \quad 1)$	$3 = 3 \cdot 1 + 0$	$C_2 \leftarrow C_2 - 3C_1$	$(0 \quad 0 \quad 1)$
On ramène le PGCD en première position :		$C_1 \leftrightarrow C_3$	$(1 \quad 0 \quad 0)$

Démonstration. Le lemme précédent donne la démonstration du théorème pour le cas $q = 1$. On peut maintenant démontrer le théorème dans le cas général par récurrence.

Supposons le résultat démontré pour un entier $q < p$ et soit $M \in \mathcal{M}_{p,q+1}(A)$ une matrice de taille $p \times (q+1)$. On note $M' \in \mathcal{M}_{p,q}(A)$ le bloc constitué par les q premières colonnes et $C \in \mathcal{M}_{p,1}(A)$ la dernière colonne. Par hypothèse de récurrence, M' admet une forme normale de Hermite $M' = U'H'$ avec $U' \in \mathrm{GL}_p(A)$ unimodulaire et $H' \in \mathcal{M}_{p,q}(A)$ triangulaire supérieure vérifiant les conditions de Hermite. Si on applique la matrice U' à $M = (M' \quad C)$, on obtient alors :

$$U'M = \begin{pmatrix} h'_{1,1} & \cdots & h'_{1,q} & c'_1 \\ 0 & \ddots & \vdots & \vdots \\ 0 & 0 & h'_{q,q} & c'_q \\ 0 & \cdots & 0 & c'_{q+1} \\ \vdots & 0 & \vdots & \vdots \\ 0 & \cdots & 0 & c'_p \end{pmatrix}.$$

En appliquant le lemme précédent, on peut trouver une matrice unimodulaire $U'' \in \mathrm{GL}_{p-q}(A)$ qui transforme le vecteur colonne $(c'_{q+1}, \dots, c'_p)$ en $(c''_{q+1}, 0, \dots, 0)$. Si on complète U'' par un bloc « identité » en une matrice $U''' = I_q \oplus U'' \in \mathrm{GL}_p(A)$, alors $U'''UM$ est presque sous forme de Hermite supérieure ; il suffit de faire encore quelque opérations (divisions euclidiennes) pour avoir $v(c'_i) < v(c'_{q+1})$ si $c'_{q+1} \neq 0$.

Enfin, si on suppose le résultat démontré pour $q \leq p$, le cas $q > p$ est immédiate, car la forme de Hermite supérieure n'impose aucune condition aux colonnes d'indice $> p$. ◇

Remarque VI.C.18. La démonstration précédente est constructive, si on a un algorithme d'Euclide constructif : il suffit d'appliquer plusieurs fois l'algorithme d'Euclide pour retrouver un analogue de l'algorithme du pivot de Gauss. (Exercice : implémenter l'algorithme !)

Exemple VI.C.19. Donnons un exemple de calcul de forme de Hermite dans l'anneau de polynômes $A = \mathbb{Q}[X]$ (qui est euclidien avec $v(P) = \deg(P)$). On considère la matrice :

$$M = \begin{pmatrix} -4X^2 & 12 + 12X - 6X^2 + 2X^3 & -6X & 6X^2 + 2X^4 \\ 8 & 16 & 0 & 0 \\ -4X - 4X^3 & 2X + 10X^2 - 6X^3 + 2X^4 & 6 - 6X^2 & 6X + 4X^3 + 2X^5 \end{pmatrix}.$$

Dans ce qui suit, le symbole $\sim$ signifiera « équivalent à gauche ». Pour appliquer l'algorithme, on travaille colonne par colonne. Sur la première colonne (en orange), le PGCD vaut 1 car la colonne contient une constante (le 8 vert). On divise cette ligne par 8 puis on l'échange avec la première pour obtenir

$$M \sim \begin{pmatrix} 1 & 2 & 0 & 0 \\ -4X^2 & 12 + 12X - 6X^2 + 2X^3 & -6X & 6X^2 + 2X^4 \\ -4X - 4X^3 & 2X + 10X^2 - 6X^3 + 2X^4 & 6 - 6X^2 & 6X + 4X^3 + 2X^5 \end{pmatrix}$$

On ajoute ensuite $4X^2L_1$ à la deuxième ligne, et $(4X^3 + 4X)L_1$ à la troisième pour avoir :

$$M \sim \begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 12 + 12X + 2X^2 + 2X^3 & -6X & 6X^2 + 2X^4 \\ 0 & 10X + 10X^2 + 2X^3 + 2X^4 & 6 - 6X^2 & 6X + 4X^3 + 2X^5 \end{pmatrix}.$$

On s'attaque maintenant à la deuxième colonne. Pour trouver le pivot, on doit calculer le PGCD des deux polynômes $P = 12 + 12X + 2X^2 + 2X^3$ et $Q = 10X + 10X^2 + 2X^3 + 2X^4$. Une brève application de l'algorithme d'Euclide étendu montre que le PGCD (qui sera notre pivot) vaut $X + 1$, avec :

$$\frac{1-X^2}{12}P+\frac{X}{12}Q=1+X.$$

Pour faire apparaître le pivot, on commence par diviser L_2 et L_3 par 12. On applique ensuite les opérations élémentaires[16] $L_3 \leftarrow L_3 - XL_2$ et $L_2 \leftarrow L_2 + XQ$, pour obtenir :

$$M \sim \begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 1+X & 0 & X^2 \\ 0 & -(X+X^2)/6 & 1/2 & (3X-X^3)/6 \end{pmatrix}.$$

Enfin, on applique $L_3 \leftarrow L_3 - XL_3/6$ pour faire disparaître les termes sous le pivot (la division euclidienne tombe forcément juste !) et obtenir :

$$M \sim \begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 1+X & 0 & X^2 \\ 0 & 0 & 1/2 & X/2 \end{pmatrix}.$$

Enfin, on multiplie la dernière ligne par 2 pour obtenir la forme de Hermite supérieure :

$$M \sim \begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 1+X & 0 & X^2 \\ 0 & 0 & 1 & X \end{pmatrix}.$$

Remarquons qu'on ne peut pas se débarrasser du 2 au-dessus du pivot $1+X$, mais on a bien $\deg(2) < \deg(1+X)$; les conditions d'Hermite sont quand même vérifiées.

Corollaire VI.C.20. Si A est un anneau euclidien, alors $\mathcal{E}_p(A) = \mathrm{GL}_p(A)$.

Démonstration. On sait déjà que $\mathcal{E}_p(A) \subset \mathrm{GL}_p(A)$. Réciproquement, supposons que $M \in \mathrm{GL}_p(A)$ est unimodulaire. Elle admet une forme d'Hermite supérieure $M = UH$ avec $U \in \mathcal{E}_p(A)$ et H triangulaire supérieure vérifiant les conditions d'Hermite. Comme $\det(M) = \det(U) \cdot \det(H)$ et que $\det(M), \det(U)$ sont inversibles, $\det(H)$ est inversible aussi. Or, $\det(H) = h_{1,1} \dots h_{p,p}$ est le produit des éléments diagonaux de H, car H est triangulaire. Chaque élément diagonal est donc lui-même inversible, donc d'après les conditions d'Hermite, tous les autres éléments hors diagonale sont nuls et H est une matrice diagonale. Elle est donc inversible, d'inverse la matrice diagonale dont les entrées sont $\left(h_{1,1}^{-1}, \dots, h_{p,p}^{-1}\right)$. On a donc bien $M \in \mathrm{GL}_p(A)$. ◇

Corollaire VI.C.21. Deux matrices à coefficients dans un anneau euclidien sont équivalentes si et seulement si elles sont élémentairement équivalentes.

Remarque VI.C.22. La forme normale de Hermite est utile pour résoudre des équations diophantiennes linéaires (c'est-à-dire des systèmes d'équations linéaires à coefficients entiers dont on cherche des solutions entières). En effet, soit $M \in \mathcal{M}_{p,q}(\mathbb{Z})$ est une matrice qui représente une équation diophantienne $MX = B$, avec $X \in \mathcal{M}_{q,1}(\mathbb{Z})$ et $B \in \mathcal{M}_{p,1}(\mathbb{Z})$. Soit $MU = H$ la forme normale d'Hermite inférieure de M. Alors $MX = B$ admet une solution si et seulement si $HY = B$ admet une solution, où $Y = U^{-1}X$. Vérifier que $HY = B$ admet une solution est facile : comme la matrice est triangulaire, on peut simplement résoudre le système par substitutions successives.

[16] Ces opérations ne sortent pas de nulle part ! Ce sont celles que l'on trouve en appliquant l'algorithme d'Euclide étendu.

§ VI.C(d) Forme normale de Smith

Théorème VI.C.23 (Forme normale de Smith). Toute matrice $M \in \mathcal{M}_{p,q}(A)$ à coefficients dans un anneau euclidien A est équivalente à une matrice D de la forme suivante :

$$D = \begin{pmatrix} d_1 & 0 & \dots & 0 & 0 \\ 0 & \ddots & 0 & 0 & 0 \\ 0 & 0 & d_r & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Le nombre r est le rang de M (vue à coefficients dans K_A) et d_i divise d_{i+1} pour tout $i \in \{1, \dots, r-1\}$. De plus, les d_i sont uniques à association (produit par un inversible) près.

Définition VI.C.24. Un triplet (U, D, V) constitué par deux matrices unimodulaires $U \in \mathrm{GL}_p(A)$, $V \in \mathrm{GL}_q(A)$ et une matrice diagonale $D \in \mathcal{M}_{p,q}(A)$ telles que $UMV = D$ est appelée *forme normale de Smith* de M. Les éléments $(d_1, \dots, d_r)$ sont appelés les *facteurs invariants* de M.

La démonstration du théorème va occuper le reste de cette section. On fixe A dans la suite.

Lemme VI.C.25. Toute matrice $M \in \mathcal{M}_{p,q}(A)$ est équivalente à une matrice de la forme :

$$N = \begin{pmatrix} n_{1,1} & 0 & \cdots & 0 \\ 0 & * & * & * \\ \vdots & * & \widetilde{N} & * \\ 0 & * & * & * \end{pmatrix}.$$

Démonstration. Soit M une matrice quelconque. On pose $i = 0$ et $N_0 = M$. Tant que N_i n'est pas sous la forme souhaitée, on répète les opérations suivantes :

i) En utilisant l'algorithme d'Euclide étendu (**Lemme VI.C.16**), on ramène par des opérations élémentaires sur les lignes N_i à une matrice N_i' sous la forme suivante, où r_i' est le PGCD des entrées de la première colonne de N_i :

$$N_i' = \begin{pmatrix} r_i' & * & \cdots & * \\ 0 & * & * & * \\ \vdots & * & \widetilde{N}_i' & * \\ 0 & * & * & * \end{pmatrix}.$$

ii) De la même manière, par des opérations sur les colonnes, on ramène N_i' à une matrice N_{i+1} sous la forme suivante, où r_{i+1} est le PGCD des entrées de la première ligne de N_i' :

$$N_{i+1} = \begin{pmatrix} r_{i+1} & 0 & \cdots & 0 \\ * & * & * & * \\ \vdots & * & \widetilde{N}_{i+1} & * \\ * & * & * & * \end{pmatrix}.$$

La suite $(v(r_0), v(r_0'), v(r_1), v(r_1'), \dots)$ est une suite décroissante d'éléments de $\mathbb{N} \cup \{-\infty\}$. En effet, r_i' divise r_i et r_{i+1} divise r_i' (à chaque fois, c'est le PGCD d'une famille de nombres qui inclut l'élément précédent). Cette suite finit donc par être stationnaire : il existe un rang i_0 tel que $v(r_{i_0}) = v(r_{i_0}') = v(r_{i_0+1})$. Mais cela signifie que r_{i_0}', qui est donc associé à r_{i_0+1}, est déjà le PGCD des éléments de la première colonne de N_{i_0}. Dans ce cas, l'algorithme d'Euclide étendu consiste simplement à éliminer les entrées des autres colonnes en leur retirant un multiple de la première, sans modifier la première colonne. La matrice N_{i_0+1} est donc bien sous la forme voulue : sa première ligne *et* sa première colonne ne contiennent qu'une entrée non nulle (la première) et l'algorithme s'y est arrêté. ◇

Lemme VI.C.26. Toute matrice $M \in \mathcal{M}_{p,q}(A)$ est équivalente à une matrice diagonale dont les $r = \mathrm{rg}(M)$ premières entrées sont non nulles, et les autres sont nulles.

Démonstration. En appliquant l'algorithme du lemme précédent $\min(p,q)$ fois (à M, puis $\widetilde{N}$, etc.) on obtient une matrice de la forme :

$$M \sim \begin{pmatrix} d_1 & 0 & 0 & 0 & 0 \\ 0 & \ddots & 0 & 0 & 0 \\ 0 & 0 & d_{\min(p,q)} & 0 & 0 \end{pmatrix}.$$

Or, les opérations élémentaires préservent le rang, donc exactement r éléments parmi les d_i sont non nuls. Quitte à échanger lignes et colonnes, on peut supposer que ces éléments non nuls sont les r premiers, $d_1, \dots, d_r$ et que $d_i = 0$ pour $i > r$. ◇

Attention, la matrice trouvée par le lemme précédent n'est pas nécessairement la forme normale de Smith, car on n'a pas encore la relation de divisibilité entre les coefficients.

Lemme VI.C.27. Toute matrice admet une forme normale de Smith.

Démonstration. Soit M une matrice. Grâce au lemme précédent, on peut supposer qu'elle est de la forme suivante :

$$M = \begin{pmatrix} d_1 & 0 & \dots & 0 & 0 \\ 0 & \ddots & 0 & 0 & 0 \\ 0 & 0 & d_r & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

On procède par récurrence sur r. Le résultat est clair pour $r = 1$. Supposons le résultat démontré pour un rang $r-1$ donné. Par opérations élémentaires sur les colonnes, M est équivalente à :

$$M \sim \begin{pmatrix} d_1 & 0 & \dots & 0 & 0 \\ \vdots & \ddots & 0 & 0 & 0 \\ d_r & 0 & d_r & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

En appliquant l'algorithme du premier lemme, on peut ramener le PGCD de tous les d_i en première position ; en particulier, il divise tous les autres éléments de la matrice. Le reste de la matrice est de rang $r-1$ et on peut donc appliquer l'hypothèse de récurrence. ◇

Définition VI.C.28. Soit $M \in \mathcal{M}_{p,q}(A)$ une matrice et $1 \leq s \leq \min(p,q)$ un entier. Un *mineur d'ordre s* de M est le déterminant d'une matrice $M' \in \mathcal{M}_{s,s}(A)$ obtenue en retirant $p-s$ lignes et $q-s$ colonnes à M. On note $\Delta_s(M)$ le PGCD de tous les mineurs d'ordre s de M.

Remarque VI.C.29. On définit souvent $\Delta_0(M) = 1$: le déterminant de l'unique matrice (vide) de $\mathcal{M}_{0,0}(A)$ est égal à 1.

Exemple VI.C.30. Pour M quelconque, $\Delta_1(M)$ est le PGCD de toutes les entrées de M.

Exemple VI.C.31. Si $M \in \mathcal{M}_p(A)$ est carrée, alors $\Delta_p(M) = \det(M)$ est le déterminant de M.

Exemple VI.C.32. Soit $M = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \in \mathcal{M}_{2,3}(\mathbb{Z})$. Alors $\Delta_2(M)$ est le PGCD des trois mineurs suivants :

$$\begin{vmatrix} 1 & 2 \\ 4 & 5 \end{vmatrix} = -3, \qquad \begin{vmatrix} 1 & 3 \\ 4 & 6 \end{vmatrix} = -6, \qquad \begin{vmatrix} 2 & 3 \\ 5 & 6 \end{vmatrix} = -3.$$

On a donc $\Delta_2(M) = 3$.

Proposition VI.C.33. Soit $M \sim N \in \mathcal{M}_{p,q}(A)$ deux matrices équivalentes. Alors pour tout $s \leq \min(p,q)$, on a $\Delta_s(M) = \Delta_s(N)$ (à association près).

Démonstration. Il suffit de traiter le cas où M et N sont équivalentes à gauche (il suffit de passer à la transposée pour l'équivalence à droite et d'utiliser la transitivité de l'égalité).

Commençons par le cas où $p = q$. Pour une matrice M quelconque, on note $M_{[j_1 \dots j_s]}^{[i_1 \dots i_s]}$ la matrice carrée obtenue en sélectionnant les lignes $(1 \leq i_1 < \cdots < i_s \leq p)$ et les colonnes $(1 \leq j_1 < \cdots < j_s \leq q)$ de la matrice M. Un petit calcul (décomposer les matrices par blocs) montre que si $N = UM$ (avec U unimodulaire), alors pour tous $(i_1 < \cdots < i_s)$ et $(j_1 < \cdots, <)$, alors on a l'égalité suivante :

$$\det\left(N_{[j_1 \dots j_s]}^{[i_1 \dots i_s]}\right) = \sum_{k_1 < \cdots < k_s} \det\left(U_{[k_1 \dots k_s]}^{[i_1 \dots i_s]}\right) \cdot \det\left(M_{[j_1 \dots j_s]}^{[k_1 \dots k_s]}\right).$$

En particulier, les diviseurs communs des mineurs d'ordre s de M divisent tous les mineurs d'ordre s de N, donc $\Delta_s(M)$ divise $\Delta_s(N)$. Comme U est unimodulaire, on a aussi $M = U^{-1}N$, donc par le même raisonnement, $\Delta_s(N)$ divise $\Delta_s(M)$. Finalement, $\Delta_s(M)$ et $\Delta_s(N)$ sont associés.

Supposons maintenant que $p > q$. On peut compléter M et $N = UM$ en des matrices carrées $\widetilde{M}, \widetilde{N}$ de taille $p \times p$ en posant :

$$\widetilde{M} = (M \quad 0), \qquad \widetilde{N} = (N \quad 0).$$

Il est clair que $\Delta_s(\widetilde{M}) = \Delta_s(M)$ et $\Delta_s(\widetilde{N}) = \Delta_s(N)$. De plus, $\widetilde{M} = U\widetilde{N}$, donc $\Delta_s(\widetilde{M}) = \Delta_s(\widetilde{N})$ par ce qui précède.

Supposons enfin que $p < q$. On peut compléter M, N, U en des matrices $\widetilde{M}, \widetilde{N}, \widetilde{U}$ de taille $q \times q$ en posant :

$$\widetilde{M} = \begin{pmatrix} M \\ 0 \end{pmatrix}, \qquad \widetilde{N} = \begin{pmatrix} N \\ 0 \end{pmatrix}, \qquad \widetilde{U} = \begin{pmatrix} U & 0 \\ 0 & I_{q-p} \end{pmatrix}.$$

Comme avant, $\Delta_s(\widetilde{M}) = \Delta_s(M)$ et $\Delta_s(\widetilde{N}) = \Delta_s(N)$, et on a de plus $\widetilde{N} = \widetilde{U}\widetilde{M}$, d'où le résultat. ◇

Corollaire VI.C.34. La forme normale de Smith d'une matrice est unique.

Démonstration. Soit M et D sa forme de Smith, une matrice diagonale d'entrées non-nulles $d_1, \dots, d_r$ telle que d_i divise d_{i+1} pour tout i. Alors pour tout $i \leq r$, on a clairement $\Delta_i(D) = d_1 \dots d_i$. On obtient donc $d_1 = \Delta_1(D)$ et $d_i = \Delta_i(D)/\Delta_{i-1}(D)$ pour $i > 1$. Comme les Δ_i sont invariants par équivalence de matrice, les facteurs invariants dans la forme de Smith sont uniquement déterminés par la matrice de départ. ◇

Exemple VI.C.35. Déterminons la forme normale de Smith de la matrice :

$$M = \begin{pmatrix} 30 & 8 & 18 \\ 2 & 3 & 1 \\ -8 & -1 & -5 \end{pmatrix} \in \mathcal{M}_3(\mathbb{Z}).$$

On commence par appliquer l'algorithme d'Euclide étendu sur la première colonne. Le PGCD des éléments de cette colonne vaut 2, qui se trouve être le deuxième élément de la colonne. On effectue donc successivement $L_2 \leftrightarrow L_1$, $L_2 \leftarrow L_2 - 15L_1$ et $L_3 \leftarrow L_3 + 4L_1$ pour obtenir :

$$M \sim \begin{pmatrix} 2 & 3 & 1 \\ 0 & -37 & 3 \\ 0 & 11 & -1 \end{pmatrix}$$

On applique maintenant l'algorithme d'Euclide étendu à la première ligne : le PGCD vaut 1, et en appliquant quelques opérations élémentaires sur les colonnes on obtient :

$$M \sim \begin{pmatrix} 1 & 0 & 0 \\ 3 & -46 & -6 \\ -1 & 14 & 2 \end{pmatrix}.$$

On remarque le PGCD (l'élément en haut à gauche) continue à diminuer. On applique une dernière fois l'algorithme d'Euclide étendu pour trouver :

$$M \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & -46 & -6 \\ 0 & 14 & 2 \end{pmatrix}.$$

On s'attaque maintenant au deuxième bloc. Le PGCD de la deuxième colonne vaut $2 = 3 \cdot (-46) + 10 \cdot 14$. Après quelques opérations élémentaires, on obtient :

$$M \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 2 \\ 0 & 0 & -4 \end{pmatrix}.$$

Il ne reste plus qu'à soustraire la deuxième colonne de la troisième, et multiplier celle-ci par -1, pour trouver :

$$M \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{pmatrix}.$$

Les facteurs invariants de M sont donc $(1, 2, 4)$. En suivant pas à pas le calcul précédent, on trouve également les matrices de passage U et V.

Remarque VI.C.36. On pourrait également calculer les facteurs invariants d'une matrice M en calculant les PGCD des mineurs $\Delta_i(M)$. Par exemple pour la matrice M de l'exemple précédent, on trouve $\Delta_1(M) = \mathrm{pgcd}(30, 8, 18, \dots) = 1$, $\Delta_2(M) = 2$ et $\Delta_3(M) = 8$. On obtient donc $d_1 = \Delta_1 = 1$, $d_2 = \Delta_2/\Delta_1 = 2$ et $d_3 = \Delta_3/\Delta_2 = 4$, comme attendu. Cette méthode est cependant rarement praticable du point de vue de la complexité. Si M est une matrice carrée de taille n,

- Calculer Δ_1 requiert le calcul du PGCD de n^2 nombres ;
- Calculer Δ_2 requiert le calcul de $\binom{n}{2}^2$ mineurs de taille 2×2, puis de leur PGCD ;
- Calculer Δ_3 requiert le calcul de $\binom{n}{3}^2$ mineurs de taille 3×3, puis de leur PGCD ;
- Et ainsi de suite jusque Δ_n qui requiert le calcul d'un PGCD de taille $n \times n$.

Si les entrées de M ont en moyenne b bits, les calculs de PGCD (par l'algorithme d'Euclide) de deux nombres sont de complexité $O(b^2)$, ce qui donne une borne supérieure pour la complexité :

$$b^2 \sum_{k=0}^{n} \binom{n}{k}^2 = b^2 \binom{2n}{n} = b^2 \frac{(2n)!}{(n!)^2} \sim b^2 \frac{2^{2n}}{\sqrt{n\pi}}.$$

À titre de comparaison, il existe des algorithmes de complexité $(bn^\alpha)^{1+o(1)}$ avec un $\alpha > 0$ connu pour calculer les facteurs invariants de la matrice.

Remarque VI.C.37. Comme on le verra dans la démonstration du théorème suivant, la forme normale de Smith est utile pour déterminer le noyau et le conoyau d'une application $\mathbb{Z}$-linéaire (entre groupes abéliens de type fini), exactement comme en algèbre linéaire où la forme $M \sim I_r \oplus 0$ joue le rôle de la forme normale de Smith.

Section VI.D. Structure des groupes abéliens de type fini

On rappelle qu'un groupe abélien G est dit de type fini s'il existe une famille finie $S = \{x_1, \dots, x_r\} \subset G$ d'éléments de G telle que $\langle x_1, \dots, x_r \rangle = G$.

Exemple VI.D.1. Les groupes abéliens finis sont de type fini (on peut prendre $S = G$). Le groupe $\mathbb{Z}$ est de type fini avec $S = \{1\}$.

Lemme VI.D.2. Le produit de deux groupes de types finis est de type fini.

Démonstration. Si G et H sont de type finis, engendrés respectivement par $\{x_1, \dots, x_r\}$ et $\{y_1, \dots, y_s\}$, alors $G \times H$ est engendré par la famille $\{(x_1, 0), \dots, (x_r, 0), (0, y_1), \dots, (0, y_s)\}$. ◇

Lemme VI.D.3. Un groupe abélien G est de type fini si et seulement s'il existe un morphisme de groupes surjectif $\varphi: \mathbb{Z}^r \to G$.

Démonstration. Si G est engendré par $\{x_1, \dots, x_r\}$, alors le morphisme $\varphi: \mathbb{Z}^r \to G$ défini par la formule suivante est surjectif :

$$\varphi(n_1, \dots, n_r) \coloneqq \sum_{i=1}^{r} n_i x_i = n_1 x_1 + \cdots + n_r x_r.$$

Réciproquement, si un tel morphisme existe, alors la famille $\{\varphi(1, 0, \dots, 0), \dots, \varphi(0, \dots, 0, 1)\}$ est finie et engendre G. ◇

Lemme VI.D.4. Tout quotient d'un groupe abélien de type fini est de type fini.

Démonstration. Si G est de type fini avec $\varphi: \mathbb{Z}^r \to G$ surjectif et si $H \leq G$ est un sous-groupe (nécessairement distingué), alors la composée $\mathbb{Z}^r \to G \to G/H$ est la composée de deux morphismes surjectifs et est donc elle-même un morphisme surjectif. ◇

Lemme VI.D.5. S'il existe un morphisme de groupes abéliens $\varphi: G \to H$ tel que $\ker(\varphi)$ et $\mathrm{im}(\varphi)$ sont de types finis, alors G est de type fini.

Démonstration. Soient $y_1 = \varphi(x_1), \dots, y_r = \varphi(x_r) \in H$ une famille génératrice de $\mathrm{im}(\varphi)$ et soit $z_1, \dots, z_s \in G$ une famille génératrice de $\ker(\varphi)$. Alors la famille $\{x_1, \dots, x_r, z_1, \dots, z_s\}$ est génératrice. En effet, soit $g \in G$ un élément quelconque. L'élément $\varphi(g)$ appartient à $\mathrm{im}(\varphi)$, donc il existe des entiers $k_1, \dots, k_r$ tels que $\varphi(g) = \sum_i k_i \varphi(x_i)$. L'élément $g - \sum_i k_i x_i$ appartient donc au noyau de φ, donc il existe des entiers $l_1, \dots, l_s$ tels que $g - \sum_i k_i x_i = \sum_j l_j z_j$ et donc finalement $g = \sum_i k_i x_i + \sum_j l_j z_j$. ◇

Proposition VI.D.6. Un sous-groupe d'un groupe abélien de type fini est également de type fini.

Remarque VI.D.7. Cela n'a absolument rien d'évident ! C'est faux si on considère des groupes non-abéliens : le groupe libre F_2 à deux générateurs x, y contient le sous-groupe $\langle yxy^{-1}, y^2xy^{-2}, y^3xy^{-3}, \dots \rangle$ qui n'est pas de type fini.

Démonstration. Soit $G = \langle x_1, \dots, x_r \rangle$ un groupe abélien de type fini et $H \lhd G$ un sous-groupe. On raisonne par récurrence sur r. Le cas $r = 0$ est évident, et si $r = 1$, alors $G = \langle x_1 \rangle \cong \mathbb{Z}$. Tous les sous-groupes de $\mathbb{Z}$ sont isomorphes à 0 ou $\mathbb{Z}$, qui sont bien de type fini.

Supposons l'énoncé démontré pour un entier $r - 1 \geq 1$. Soit $K = \langle x_1, \dots, x_{r-1} \rangle$ le sous-groupe de G engendré par les $r - 1$ premiers générateurs et soit $\pi: G \to G/K$ le quotient, qui est engendré par la

classe de x_r. Le quotient induit une application $\pi|_H : H \to H/K$. Son image est un sous-groupe de G/K, qui est engendré par un unique élément et est donc soit trivial, soit isomorphe à $\mathbb{Z}$, donc H/K est lui-même trivial ou isomorphe à $\mathbb{Z}$. De plus, son noyau $\ker(\pi|_H)$ est un sous-groupe de K, qui est engendré par $r-1$ éléments. On peut donc appliquer l'hypothèse de récurrence pour voir que $\ker(\pi|_H)$ est de type fini. En appliquant le lemme précédent, on conclut que H est de type fini. ◇

Définition VI.D.8. Un groupe abélien est dit *libre (de type fini)* s'il est isomorphe à un produit fini de copies de $\mathbb{Z}$. Si G est abélien libre de type fini, on appelle *base* de G une famille $(e_1, \dots, e_r)$ d'éléments de G telle que le morphisme induit $\mathbb{Z}^r \to G$ est un isomorphisme.

Remarque VI.D.9. En principe, le nombre r pourrait dépendre de la base. Mais comme pour les espaces vectoriels, on va démontrer que ce n'est pas le cas.

La proposition suivante (dont la preuve est claire) nous indique que l'étude des morphismes entre groupes abélien libres de type fini se ramène à quelque chose qui ressemble à de l'algèbre linéaire.

Proposition VI.D.10. Soit $G \cong \mathbb{Z}^p$ et $H \cong \mathbb{Z}^q$ deux groupes abéliens libres de type fini, et soit $(e_1, \dots, e_p)$, $(f_1, \dots, f_q)$ des bases respectivement de G et H. Il y a une bijection entre les morphismes de groupes $G \to H$ et les éléments de $\mathcal{M}_{q,p}(\mathbb{Z})$, définie par :

$$\mathcal{M}_{q,p}(\mathbb{Z}) \to \mathrm{Mor}(G,H), \qquad M \mapsto \varphi_M.$$

Le morphisme $\varphi_M : G \to H$ associé à une matrice $M \in \mathcal{M}_{q,p}(\mathbb{Z})$ est caractérisé par :

$$\forall 1 \le i \le r, \qquad \varphi_M(e_i) = \sum_{j=1}^{q} M_{j,i} f_j.$$

De plus, on a $\varphi_{MN} = \varphi_M \varphi_N$ pour toute paire de matrice composables.

Remarque VI.D.11. Reprenons les notations de la proposition et soit $x \in G$ un élément, de « coordonnées » $(x_1, \dots, x_p) \in \mathbb{Z}^p$ – c'est-à-dire que $x = x_1 e_1 + \cdots + x_p e_p$. Alors les « coordonnées » de $\varphi_M(x) \in H$, c'est-à-dire les coefficients $(y_1, \dots, y_q) \in \mathbb{Z}^q$ tels que $\varphi_M(x) = y_1 f_1 + \cdots + y_q f_q$, vérifient l'équation matricielle attendue :

$$\begin{pmatrix} y_1 \\ \vdots \\ y_q \end{pmatrix} = M \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}.$$

Théorème/Définition VI.D.12. Toutes les bases d'un groupe abélien libre de type fini G ont le même nombre d'éléments. Ce nombre est appelé le *rang* de G.

Démonstration. Soit $(e_1, \dots, e_r)$ et $(f_1, \dots, f_s)$ deux bases de G. Il suffit de montrer que $r \le s$ (par symétrie, on aura alors $s \le r$). L'identité de G correspond à une matrice $M \in \mathcal{M}_{s,r}(\mathbb{Z})$, dont les coefficients sont les uniques nombres qui vérifient $\varphi_M = \mathrm{id}$, c'est-à-dire, pour tout $1 \le i \le r$, $e_i = \sum_{j=1}^{s} M_{j,i} f_j$.

La matrice M admet une forme normale de Smith : il existe des matrices unimodulaires $U \in \mathrm{GL}_s(\mathbb{Z})$ et $V \in \mathrm{GL}_r(\mathbb{Z})$ et une matrice diagonale $D = \mathrm{diag}(d_1, \dots, d_{\min(r,s)})$ (et $d_k = 0$ pour $k > \min(r,s)$) telles que $UMV = D$.

Notons $\vec{e} = (e_1, \dots, e_r) \in \mathcal{M}_{1,r}(G)$ le « vecteur à coefficients dans G » formé par les e_i, et de la même manière notons $\vec{f} = (f_1, \dots, f_s) \in \mathcal{M}_{1,s}(G)$. L'équation ci-dessus se réécrit $\vec{e} = \vec{f} M$. Comme $D = UMV$,

on obtient $\vec{e}V = \vec{f}U^{-1}D$. Les matrices U et V étant inversibles, les deux familles suivantes forment encore des bases de G :

$$(\tilde{e}_1, \dots, \tilde{e}_s) \coloneqq \vec{e}V, \qquad \left(\tilde{f}_1, \dots, \tilde{f}_r\right) \coloneqq \vec{f}U^{-1}.$$

L'équation $\vec{e}V^{-1} = \vec{f}UD$ devient alors, pour tout k :

$$\tilde{e}_k = d_k \tilde{f}_k.$$

Or, $d_k = 0$ pour $k > \min(r, s)$, donc pour que la famille $\vec{e}V^{-1}$ forme une base, il faut avoir $s \leq r$. ◇

Théorème VI.D.13. Soit G un groupe abélien libre de type fini et $r \in \mathbb{N}$ son rang. Soit $H \leq G$ un sous-groupe de G. Alors H est libre de type fini, avec pour rang $s \leq r$. De plus, il existe des entiers $d_1 | \dots | d_s$ et une base $(e_1, \dots, e_r)$ de G tels que $(d_1 e_1, \dots, d_s e_s)$ forme une base de H.

Démonstration. Soit $(g_1, \dots, g_r)$ une base de G et $(h_1, \dots, h_k)$ une famille génératrice de H. Comme avant, on peut écrire $h_j = \sum_{i=1}^{r} x_i M_{i,j}$. La matrice M admet une forme normale de Smith, $D = UMV$ avec $D = \mathrm{diag}(d_1, \dots, d_s)$. Dans la base $\vec{e} = \vec{g}V$, la famille génératrice $\vec{f} = \vec{h}U^{-1}$ devient $(d_1 e_1, \dots, d_s e_s, 0, \dots, 0)$, d'où le résultat. ◇

On en arrive enfin au théorème principal de ce chapitre, qui conclut le cours :

Théorème VI.D.14 (Structure des groupes abéliens de type fini). Soit G un groupe abélien de type fini. Il existe des entiers $r, s \geq 0$ et des entiers naturels $d_1 | d_2 | \dots | d_s$ tels que l'on ait l'isomorphisme :

$$G \cong \mathbb{Z}^r \times \prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}.$$

De plus, les entiers r, s et $d_1, \dots, d_s$ sont uniquement déterminés par G.

Définition VI.D.15. Le nombre r dans la décomposition du théorème s'appelle le *rang* du groupe G. Les nombres $d_1 | \dots | d_s$ sont appelés ses *facteurs invariants*.

Remarque VI.D.16. Cette notion de rang coïncide avec la définition en termes de cardinal d'une base pour les groupes abéliens libres.

Remarque VI.D.17. Un résultat similaire existe en remplaçant $\mathbb{Z}$ par un anneau principal A et les groupes abéliens par les A-modules.

Démonstration. Pour démontrer l'existence, il suffit d'appliquer le théorème précédent au noyau $\ker(\varphi)$ d'un morphisme surjectif $\varphi : \mathbb{Z}^n \to G$. Il existe une base $(e_1, \dots, e_n)$ de $\mathbb{Z}^n$ tel que $\ker(\varphi)$ admette $(d_1 e_1, d_2 e_2, \dots, d_s e_s)$ pour base. L'image G est alors isomorphe à :

$$(\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z}) \times \dots \times (\mathbb{Z}/d_s\mathbb{Z}) \times (\mathbb{Z}/0) \times \dots \times (\mathbb{Z}/0).$$

Quitte à éliminer les éventuels premiers facteurs invariants d_i qui vaudraient 1 (et qui disparaissent dans le quotient : $\mathbb{Z}/1\mathbb{Z} = 0$), on retrouve bien la forme du théorème.

Pour démontrer l'unicité, considérons le sous-groupe de torsion :

$$T \coloneqq \{\, x \in G \mid \exists n \in \mathbb{N}^*,\ nx = 0 \,\}.$$

Quelle que soit la décomposition, ce sous-groupe T est égal au facteur $\prod_{i=1}^{s}(\mathbb{Z}/d_i\mathbb{Z})$ et donc G/T est isomorphe à la partie libre de la décomposition. Comme le rang d'un groupe abélien libre de type fini ne dépend que du groupe en question, et que T ne dépend que de G, on en déduit que G détermine r.

Il nous reste à démontrer que les facteurs invariants ne dépendent pas de la décomposition, c'est-à-dire qu'on peut les retrouver à partir de données qui ne dépendent que du groupe. Soit $p_1, \dots, p_k$ les facteurs premiers de d_s. Comme $d_i | d_s$ pour tout i, l'ensemble des facteurs premiers de d_i est un sous-ensemble de $\{p_1, \dots, p_k\}$, de telle sorte que l'on peut écrire, où $0 \leq \alpha_{1,j} \leq \alpha_{2,j} \leq \cdots \leq \alpha_{s,j}$ pour tout $1 \leq j \leq k$:

$$d_i = \prod_{j=1}^{k} p_j^{\alpha_{i,j}} = p_1^{\alpha_{i,1}} \dots p_k^{\alpha_{i,k}}.$$

D'après le théorème des restes chinois, on a :

$$T = \prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z} = \prod_{i=1}^{s} \prod_{j=1}^{k} \mathbb{Z}/p_j^{\alpha_{i,j}}\mathbb{Z}.$$

Comme G est abélien, il admet un unique p-sous-groupe de Sylow (car il est nécessairement distingué). Quitte à se restreindre à ce sous-groupe, on peut donc supposer que $k = 1$ et que l'on a (avec $p = p_1$ et $\alpha_1 \leq \cdots \leq \alpha_s$) :

$$T = \mathbb{Z}/p^{\alpha_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{\alpha_s}\mathbb{Z}.$$

Étant donné un entier $\beta \geq 1$, on note $T_\beta = \{ p^\beta x \mid x \in T \} \leq T$ (qui ne dépend que de G). Un calcul rapide montre que le cardinal de T_β est égal à :

$$|T_\beta| = p^{\min(0,\alpha_1-\beta)} \dots p^{\min(0,\alpha_s-\beta)} = \prod_{i \text{ t.q. } \alpha_i > \beta} p^{\alpha_i - \beta}.$$

En particulier, on a :

$$\frac{|T_\beta|}{|T_{\beta+1}|} = p^{c(\beta)}, \qquad c(\beta) \coloneqq |\{ i \mid \alpha_i > \beta \}|.$$

Ces nombres ne dépendent que de G, et ils permettent de retrouver les valeurs des nombres α_i. La donnée des nombres α_i, et donc les facteurs invariants de G, ne dépendent ainsi que de G. ◇

Corollaire VI.D.18. Si A est un groupe abélien de type fini est sans torsion, alors il est libre.

Remarque VI.D.19. Ce corollaire est faux sans l'hypothèse de finitude. Par exemple, $(\mathbb{Q}, +)$ est un groupe abélien sans torsion, mais il n'est pas libre.

Exemple VI.D.20. Soit G le quotient de $\mathbb{Z}^3$ par le sous-groupe engendré par les vecteurs $x_1 = (3, -2, 1)$ et $x_2 = (2, 0, 2)$. Quel est son rang, ses facteurs invariants ? Étant donné un vecteur, comment le représenter dans la décomposition canonique de G ? On considère la matrice :

$$M = \begin{pmatrix} x_1 & x_2 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ -2 & 0 \\ 1 & 2 \end{pmatrix} \in \mathcal{M}_{3,2}(\mathbb{Z}).$$

Le groupe G est le quotient de $\mathbb{Z}^3$ par l'image du morphisme de groupes :

$$\mathbb{Z}^2 \to \mathbb{Z}^3, \qquad \begin{pmatrix} k_1 \\ k_2 \end{pmatrix} \mapsto M \cdot \begin{pmatrix} k_1 \\ k_2 \end{pmatrix}.$$

La matrice M admet une décomposition de Smith $D = UMV$ avec :

$$U = \begin{pmatrix} 1 & 1 & 0 \\ 2 & 3 & 0 \\ -1 & -1 & 1 \end{pmatrix}, \qquad D = \begin{pmatrix} 1 & 0 \\ 0 & 4 \\ 0 & 0 \end{pmatrix}, \qquad V = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}.$$

Donc à changement de bases près, le morphisme ci-dessus est équivalent au morphisme donné par :

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \mapsto \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} 0 \\ 4 \\ 0 \end{pmatrix}.$$

L'image de ce morphisme est $\mathbb{Z} \times 4\mathbb{Z} \times 0$, donc G est isomorphe à :

$$\mathbb{Z}/\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/0 = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}.$$

Il est donc de rang 1, et son unique facteur invariant est $d_1 = 4$.

Pour trouver un représentant d'un vecteur $g = [g_1, g_2, g_3] \in G$ quelconque (initialement représenté par un élément de $\mathbb{Z}^3/\langle x_1, x_2 \rangle$), on lui applique la transformation U et on réduit ses coordonnées modulo les éléments de la diagonale étendue de D. Par exemple, le vecteur $w = (8, -5, 3)$ se représente ainsi :

$$\begin{pmatrix} 8 \\ -5 \\ 3 \end{pmatrix} \mapsto U \cdot \begin{pmatrix} 8 \\ -5 \\ 3 \end{pmatrix} = \begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix} \mapsto \begin{pmatrix} 3 \bmod 1 \\ 1 \bmod 4 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \in \prod \begin{matrix} 0 \\ \mathbb{Z}/4\mathbb{Z} \\ \mathbb{Z} \end{matrix}.$$

On vérifie que le vecteur w est bien d'ordre 4 dans G : on a $4w = 10x_1 + x_2$.

BIBLIOGRAPHIE

[1] W. R. Alford, A. Granville, et C. Pomerance, « There are Infinitely Many Carmichael Numbers ». In: *Ann. of Math.* **139**.3 p. 703 (1994), DOI:10.2307/2118576, ISSN: 0003486X.
[2] T. H. Cormen, C. E. Leiserson, R. R. Rivest, et C. Stein, *Introduction à l'algorithmique: cours et exercices*. (2e édition) Paris: Dunod (2004), ISBN: 978-2-10-003922-7.
[3] O. Debarre, Algèbre II (2012).
[4] T. C. Hull, *Origametry: Mathematical Methods in Paper Folding*. (1re édition) Cambridge University Press (2020), DOI:10.1017/9781108778633, ISBN: 978-1-108-77863-3.
[5] K. Ireland et M. Rosen, *A Classical Introduction to Modern Number Theory*. Graduate Texts in Mathematics, New York, NY: Springer New York (1990), DOI:10.1007/978-1-4757-2103-4, ISBN: 978-1-4419-3094-1.
[6] S. Lang, *Algèbre*. (3e édition) Paris: Dunod (2020), ISBN: 978-2-10-081471-8.
[7] I. M. Niven, H. S. Zuckerman, et H. L. Montgomery, *An introduction to the theory of numbers*. (5th ed édition) New York: Wiley (1991), ISBN: 978-0-471-62546-9.
[8] D. Perrin, *Cours d'algèbre*. CAPES-agrég mathématiques, Paris: Ellipses (1996), ISBN: 978-2-7298-5552-9.
[9] C. Pomerance, J. L. Selfridge, et S. S. Wagstaff, « The pseudoprimes to $25 \cdot 10^9$ ». In: *Math. Comp.* **35**.151 p. 1003-1026 (1980), DOI:10.1090/S0025-5718-1980-0572872-7, ISSN: 0025-5718, 1088-6842.
[10] A. Schönhage et V. Strassen, « Schnelle Multiplikation großer Zahlen ». In: *Computing* **7**.3-4 p. 281-292 (1971), DOI:10.1007/BF02242355, ISSN: 0010-485X, 1436-5057.
[11] R. Solovay et V. Strassen, « A Fast Monte-Carlo Test for Primality ». In: *SIAM J. Comput.* **6**.1 p. 84-85 (1977), DOI:10.1137/0206006, ISSN: 0097-5397, 1095-7111.
[12] Wolfram, The Wolfram Language: Fast Introduction for Programmers, https://www.wolfram.com/language/fast-introduction-for-programmers/.

INDEX