Unsere Allergrößten, wie Archimedes, Newton, Gauß,
haben stets Theorie und Anwendung gleichmäßig umfaßt.
Felix Klein, *Elementarmathematik vom höheren Standpunkt aus*, 1908

CHAPITRE IX

Le pgcd et l'algorithme d'Euclide-Bézout

Objectifs

Ce chapitre reprend l'arithmétique des nombres entiers, notamment l'algorithme d'Euclide et ses nombreuses ramifications. C'est une relecture de l'arithmétique sous un aspect algorithmique : structures algébriques sous-jacentes, preuve de correction, analyse de complexité.

C'est aussi une étape charnière pour l'algèbre, dont les chapitres suivants traiteront différents aspects. On parlera plus en détail des anneaux quotients $\mathbb{Z}_n$ au chapitre X, de la primalité et de la factorisation d'entiers au chapitre XI, on implémentera le corps des fractions $\mathbb{Q}$ au chapitre XII, suivi de l'anneau $\mathbb{Z}[i]$ dans le projet XII et des anneaux des polynômes au chapitre XIII.

Implémentation. — Afin de réaliser des implémentations complexes, songez à distribuer le travail en équipe puis à mutualiser vos solutions. Le but sera de réunir les fonctions d'intérêt général dans le fichier `integer.cc` commencé en chapitre II. Vous obtenez ainsi une mini-bibliothèque portant sur l'arithmétique des entiers. Les implémentations continueront tout au long des chapitres suivants. Comme d'habitude il convient de bien tester et commenter vos implémentations, d'autant plus en vue d'une réutilisation.

Sommaire

Approfondissement. — L'annexe IX résume brièvement le vocabulaire des anneaux commutatifs qui sera essentiel pour la suite. On saisit l'occasion de souligner quelques aspects algorithmiques et de préparer ainsi nos futures implémentations d'anneaux plus généraux. Le projet IX présente l'algorithme de Gauss-Bézout pour la résolution de systèmes d'équations linéaires sur $\mathbb{Z}$. On en déduit le théorème des diviseurs élémentaires et la classification des groupes abéliens finiment engendrés.

1. Structure de l'anneau $\mathbb{Z}$

1.1. Structure d'anneau factoriel. Le théorème fondamental de l'arithmétique dit que tout entier positif a s'exprime de manière unique comme produit de nombres premiers positifs :

$$a = 2^{v_2} \cdot 3^{v_3} \cdot 5^{v_5} \cdot 7^{v_7} \cdots = \prod_{p \text{ premier}} p^{v_p}$$

avec des exposants $v_p = v_p(a) \in \mathbb{N}$ dont tous sauf un nombre fini sont nuls. Pour le plus grand commun diviseur (pgcd) et le plus petit commun multiple (ppcm) on obtient alors

$$\operatorname{pgcd}(a,b) = \prod_{p \text{ premier}} p^{\min(v_p(a),v_p(b))} \qquad \text{et} \qquad \operatorname{ppcm}(a,b) = \prod_{p \text{ premier}} p^{\max(v_p(a),v_p(b))}.$$

Bien que ces deux formules soient importantes d'un point de vue théorique, elles n'offrent pas de solution efficace pour le calcul du pgcd ou du ppcm : pour ce faire il faudrait d'abord factoriser a et b. Or, pour les grands entiers, la factorisation est un problème très dur, dont on ne connaît pas de méthode rapide (nous y reviendrons au chapitre XI). Heureusement pour le pgcd il existe un algorithme très efficace, l'algorithme d'Euclide, qui évite entièrement le problème de factorisation.

1.2. Structure d'anneau euclidien. Étant donnés $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$ il existe $q, r \in \mathbb{Z}$ tels que $a = bq + r$ et $|r| < |b|$. Ceci est appelé une *division euclidienne* avec quotient q et reste r. Le couple (q,r) n'est en général pas unique : pour $a = 22$ et $b = 9$, par exemple, on a $a = 2b + 4 = 3b - 5$. (On a toujours deux solutions : l'une avec $q = \lfloor \frac{a}{b} \rfloor$, l'autre avec $q = \lceil \frac{a}{b} \rceil$; elles coïncident si et seulement si b divise a dans $\mathbb{Z}$ avec reste $r = 0$.) Cette ambiguïté n'est pas gênante d'un point de vue mathématique, mais pour une implémentation sur ordinateur il faut bien fixer un choix. Précisons d'abord les exigences générales.

Définition 1.1. Soit A un anneau commutatif. Une *division euclidienne* sur A est la donnée
– d'une fonction $\nu : A \to \mathbb{N}$ vérifiant $\nu(a) = 0$ si et seulement si $a = 0$, et
– d'une application $\delta : A \times A^* \to A \times A$, $(a,b) \mapsto (q,r)$ telle que $a = bq + r$ et $\nu(r) < \nu(b)$.
Dans ce cas on appelle ν un *stathme euclidien*, et δ une *division euclidienne* par rapport au stathme ν.

Définition 1.2. Un anneau A est dit *euclidien* s'il est intègre et admet une division euclidienne.

D'après ce qui précède, $\mathbb{Z}$ est euclidien par rapport au stathme $\nu(a) = |a|$. Quant à la division euclidienne δ, on a une infinité de choix possibles. Les conventions suivantes semblent les plus utiles : elles choisissent les quotients $q = \lceil \frac{a}{b} \rfloor$, $q = \lfloor \frac{a}{b} \rfloor$, $q = \lceil \frac{a}{b} \rceil$, et $q = \lfloor \frac{a}{b} \rceil$ respectivement.

Exercice/P 1.3. Pour les types entiers en C++ l'opération `a/b` donne $\lceil \frac{a}{b} \rfloor$, la partie entière du quotient, appelé quotient « tronqué », ou encore « arrondi vers zéro ». Par exemple `5/3` vaut `1` et `5%3` vaut `2`, ainsi que `(-5)/3` vaut `-1` et `(-5)%3` vaut `-2`. Par conséquent le reste `a%b` est ou zéro ou du même signe que `a`. Cette convention a été adoptée également pour la classe `Integer`. Le vérifier sur des exemples.

Optimisation. — Très souvent on veut calculer le quotient `q` et le reste `r` en même temps. Bien sûr on pourrait écrire `q=a/b` puis `r=a%b`, mais ceci effectue deux fois la même division (expliquer pourquoi). Dans ce cas il est plus efficace de n'effectuer qu'une seule division euclidienne $(a,b) \mapsto (q,r)$ comme suit :

```
void tdiv( const Integer& a, const Integer& b, Integer& q, Integer& r )
{ mpz_tdiv_qr( q.get_mpz_t(), r.get_mpz_t(), a.get_mpz_t(), b.get_mpz_t() ); }
Integer tdiv( const Integer& a, const Integer& b )
{ return a/b; }
Integer tmod( const Integer& a, const Integer& b )
{ if( b == 0 ) return a; else return a%b; }
```

Au lieu des opérateurs `/` et `%` on peut aussi utiliser deux fonctions `tdiv` et `tmod`. Ceci permet de rectifier un petit défaut de l'opérateur `%`, à savoir que `tmod(a,0)` est toujours bien défini, bien que `tdiv(a,0)` ne le soit pas. (Expliquer pourquoi c'est mathématiquement raisonnable.)

Exercice/P 1.4. On peut définir une deuxième division euclidienne en choisissant l'unique couple (q,r) avec $a = bq + r$ et $0 \leq r < |b|$. Dans ce cas nous écrivons $q = a \operatorname{div} b$ et $r = a \bmod b$; c'est la division euclidienne avec *reste positif*, usuelle en mathématique. L'implémenter sous la forme

```
void    pdiv( const Integer& a, const Integer& b, Integer& q, Integer& r );
Integer pdiv( const Integer& a, const Integer& b );
Integer pmod( const Integer& a, const Integer& b );
```

De la même manière on pourra définir et implémenter la division euclidienne avec *reste négatif* :

```
void    ndiv( const Integer& a, const Integer& b, Integer& q, Integer& r );
Integer ndiv( const Integer& a, const Integer& b );
Integer nmod( const Integer& a, const Integer& b );
```

Indication. — Dans le souci d'efficacité on pourra commencer par `tdiv(a,b,q,r)` puis corriger `q` et `r`. Vous pouvez aussi consulter la documentation via `info gmp` pour vous informer sur les fonctions `fdiv` et `cdiv` de la bibliothèque GMP.

Exercice/P 1.5. Une façon économique de choisir (q,r) est d'exiger $a = bq + r$ avec $|r| \leq \frac{1}{2}|b|$: c'est la division avec *reste symétrique*. Vérifier qu'elle *minimise* $|r|$. L'implémenter sous la forme

```
void    sdiv( const Integer& a, const Integer& b, Integer& q, Integer& r );
Integer sdiv( const Integer& a, const Integer& b );
Integer smod( const Integer& a, const Integer& b );
```

Remarque. — La définition laisse un choix seulement dans le cas où $b = 2n$ et $r = \pm n$. Afin de résoudre cette dernière ambiguïté, on pourra choisir l'unique couple (q,r) avec q pair.

2. Le pgcd et l'algorithme d'Euclide

2.1. Définition du pgcd. Rappelons la définition du pgcd en dû détail :

Définition 2.1. On dit que d *divise* a dans $\mathbb{Z}$, noté $d \mid a$, s'il existe $d' \in \mathbb{Z}$ de sorte que $dd' = a$. On dit que c est un diviseur commun de $a_1, \dots, a_n$ dans $\mathbb{Z}$ si $c \mid a_k$ pour tout k. On dit que d est un *plus grand commun diviseur* de $a_1, \dots, a_n$ s'il est un diviseur commun et que tout autre diviseur commun c divise aussi d.

Attention. — Le pgcd n'est pas unique : si d est un pgcd de $a_1, \dots, a_n$, alors $-d$ en est un autre. Cette ambiguïté fait qu'il faut dire correctement *un* pgcd et non *le* pgcd. Pour nos futures implémentations ceci pose un problème de spécification. Heureusement dans l'anneau $\mathbb{Z}$ l'ambiguïté se limite au signe. On peut s'en tirer en choisissant *le pgcd positif* pour pgcd préféré, ce qui rend la définition univoque.

Remarque 2.2. Le pgcd jouit des propriétés suivantes (les montrer) :
- Si $a = bq + r$ alors $\operatorname{pgcd}(a,b) = \operatorname{pgcd}(b,r)$ car $c|a \;\&\; c|b \iff c|b \;\&\; c|r$.
- Pour tout $a \in \mathbb{Z}$ on a $\operatorname{pgcd}(a,0) = \operatorname{pgcd}(a) = |a|$.
- On a $\operatorname{pgcd}(a_1, a_2, \dots, a_n) = \operatorname{pgcd}(a_1, \operatorname{pgcd}(a_2, \dots, a_n))$.
  Il suffit donc de savoir calculer le pgcd de deux entiers.

2.2. L'algorithme d'Euclide. Rappelons l'algorithme d'Euclide comme il est typiquement formulé dans un cours d'algèbre. Étant donnés deux entiers a, b on construit une suite finie (r_i) de la manière suivante : comme valeurs initiales on pose $r_0 = a$ et $r_1 = b$. Tant que $r_i \neq 0$ on définit r_{i+1} par une division euclidienne $r_{i-1} = r_i q_i + r_{i+1}$ avec $|r_{i+1}| < |r_i|$. Finalement $r_{n+1} = 0$, donc la dernière division $r_{n-1} = r_n q_n$ est exacte. On vérifie aisément que r_n est un pgcd de a et b, donc $|r_n|$ est le pgcd positif cherché.

Pour l'implémentation il est inutile de stocker toute la suite $r_0, r_1, \dots, r_n$; il suffit à chaque moment de travailler avec les deux derniers éléments r_{i-1} et r_i. Voici un tel algorithme « prêt à programmer » :

Algorithme IX.1 Calcul du pgcd de deux entiers selon Euclide

Entrée: deux entiers a et b

Sortie: le pgcd positif de a et b

tant que $b \neq 0$ **faire** division euclidienne $(q,r) \leftarrow \delta(a,b)$, puis affecter $a \leftarrow b$ et $b \leftarrow r$
si $a \geq 0$ **alors retourner** a **sinon retourner** $-a$

Proposition 2.3. *L'algorithme IX.1 est correct.*

DÉMONSTRATION. Notons $a_0 = a$ et $b_0 = b$ les valeurs initiales, puis a_k et b_k les valeurs des variables a et b après la $k$ième itération.

Terminaison : Soit $\nu \colon \mathbb{Z} \to \mathbb{N}$ un stathme pour la division euclidienne δ utilisée ici : par définition on a $\nu(b_0) > \nu(b_1) > \nu(b_2) > \dots$. Comme c'est une valeur dans $\mathbb{N}$, ceci ne peut durer éternellement. On arrive donc à $\nu(b_n) = 0$ après un certain nombre n d'itérations. À ce moment-là la boucle s'arrête avec $b_n = 0$.

Correction : Si $a = bq + r$ alors $\operatorname{pgcd}(a,b) = \operatorname{pgcd}(b,r)$. Autrement dit, le pgcd est préservé lors de chaque itération de la boucle. Ainsi on obtient $\operatorname{pgcd}(a_0,b_0) = \operatorname{pgcd}(a_1,b_1) = \cdots = \operatorname{pgcd}(a_n,b_n) = \operatorname{pgcd}(a_n,0) = |a_n|$. L'algorithme renvoie donc le pgcd cherché. □

Exercice/P 2.4. Implémenter une fonction `Integer pgcd( Integer a, Integer b )`. Motiver le mode de passage des paramètres. On souhaiterait normaliser le pgcd à la fin de sorte qu'il soit toujours positif ou nul. Pour visualiser le comportement de cet algorithme et pour compter le nombre d'itérations effectuées, vous pouvez faire afficher les calculs intermédiaires. Testez votre fonction sur des entiers de plus en plus grands ; combien d'itérations faut-il environ ?

Exemple 2.5. Calculer le pgcd de $a = 33! + 1$ et $b = 32! + 1$. Peut-on trouver aussi facilement le pgcd via la décomposition en facteurs premiers ? Pour information, les factorisations sont

$$33! + 1 = 101002716748738111 \cdot 143446529 \cdot 175433 \cdot 50989 \cdot 67 \qquad \text{et}$$
$$32! + 1 = 2889419049474073777 \cdot 61146083 \cdot 652931 \cdot 2281.$$

Justifier la supériorité de l'algorithme d'Euclide par rapport au calcul du pgcd via factorisation.

2.3. Analyse de complexité. Rappelons que pour a,b vérifiant $\mathrm{len}(a),\mathrm{len}(b)\leq\ell$ la division euclidienne nécessite un temps $O(\ell^2)$ avec la méthode scolaire, voire $O^+(\ell)$ avec des méthodes sophistiquées. Par construction la suite des restes successifs vérifie $|r_1|>|r_2|>\cdots>|r_n|>|r_{n+1}|=0$. Le coût total de l'algorithme d'Euclide appliqué au couple (a,b) est donc d'ordre $O(n\ell^2)$, voire $O^+(n\ell)$. Que peut-on dire du nombre n d'itérations nécessaires ?

Exercice/M 2.6. En utilisant la division euclidienne avec reste minimal, on a $|r_{i+1}|\leq\frac{1}{2}|r_i|$. En déduire que $n\leq\ell$, donc cet algorithme d'Euclide est de complexité $O(\ell^3)$, voire $O^+(\ell^2)$.

Remarque 2.7. Pour une analyse plus fine voir Gathen-Gerhard [**11**], §3.3. Il se trouve que la complexité est $O(\ell^2)$ même avec la division scolaire. Dans [**11**], §11.1 vous trouverez un raffinement de complexité $O^+(\ell)$ seulement !

Exercice/M 2.8. Expliciter une division euclidienne $(a,b)\mapsto(q,r)$ qui *maximise* $|r|$. L'algorithme d'Euclide aboutit-il toujours à trouver le pgcd ? Quelle est sa complexité dans le pire des cas ? (Voir `euclide.cc` .)

Exercice/M 2.9. En utilisant `pmod` ou `tmod`, montrer que $|r_{i+2}|<\frac{1}{2}|r_i|$ pour tout $i\geq1$. En déduire que $n\leq2\,\mathrm{len}(b)\leq2\ell$, donc la complexité est au plus un facteur deux plus grande qu'avec `smod`.

Exercice/M 2.10. On peut expliciter le pire cas de l'algorithme d'Euclide utilisant la division euclidienne avec reste positif. La suite de Fibonacci $(f_k)_{k\in\mathbb{N}}$ est définie par $f_0=1$, $f_1=1$ puis $f_{k+2}=f_{k+1}+f_k$. Les premiers termes sont $1,1,2,3,5,8,13,21,34,\ldots$

(1) Montrer que pour $a=f_{n+1}$ et $b=f_n$ l'algorithme d'Euclide nécessite exactement n itérations. Réciproquement, si pour $a>b\geq0$ l'algorithme d'Euclide nécessite n itérations, alors $a\geq f_{n+1}$ et $b\geq f_n$.

(2) En déduire que l'usage de `smod` est plus efficace que `pmod` dans l'algorithme d'Euclide.

(3) Montrer la formule close $f_n=(\lambda_+^{n+1}-\lambda_-^{n+1})/\sqrt{5}$ avec $\lambda_\pm=(1\pm\sqrt{5})/2$, et en déduire le théorème de Lamé : pour la division euclidienne avec reste positif le nombre d'itérations dans l'algorithme d'Euclide est majoré par $5\,\mathrm{len}_{10}(b)$.

Exercice/P 2.11. Un théorème de Dirichlet affirme que deux entiers a,b « aléatoires » sont premiers entre eux avec probabilité $6/\pi^2\approx60\%$. Pour vérification empirique vous pouvez écrire un programme qui parcourt $(a,b)\in[\![1,N]\!]^2$ et compte les couples vérifiant $\mathrm{pgcd}(a,b)=1$. Que trouvez-vous pour $N=10$? $N=100$? $N=1000$? $N=10000$?

Analogie. — Imaginez une « forêt mathématique » formée d'une infinité d'arbres très fins, avec un arbre planté à chaque position du réseau $\mathbb{Z}^2$ dans le plan $\mathbb{R}^2$. Vous êtes à l'origine. Quelle fraction d'arbres voyez-vous ?

2.4. Bézout ou Euclide étendu. Rappelons une propriété principale de l'anneau $\mathbb{Z}$:

Proposition 2.12. *Tout sous-groupe I de $(\mathbb{Z},+)$ est de la forme $I=a\mathbb{Z}$ pour un entier $a\in\mathbb{Z}$.*

DÉMONSTRATION. Si $I=\{0\}$ alors $I=0\mathbb{Z}$ et on prend $a=0$. Sinon on a $I\neq\{0\}$, il existe donc $a\in I$ avec $a\neq0$. On choisit a avec $|a|$ minimal. Comme $-a\in I$, on peut supposer que $a>0$. Comme I est un sous-groupe, on a déjà $I\supset a\mathbb{Z}$. Réciproquement, pour $x\in I$ quelconque on considère la division euclidienne par a : il existe $q,r\in\mathbb{Z}$ tels que $x=qa+r$ et $|r|<a$. Avec $a\in I$ on a aussi $qa\in I$ et donc $r=x-qa\in I$. Notre choix minimal de a veut dire que $|r|<a$ n'est possible que pour $r=0$, donc x est un multiple de a, autrement dit $x\in a\mathbb{Z}$. On conclut que $I=a\mathbb{Z}$. □

Proposition 2.13. *Pour tout couple $a,b\in\mathbb{Z}$ on a $a\mathbb{Z}+b\mathbb{Z}=d\mathbb{Z}$ où d est un pgcd de a et b. Il existe donc $u,v\in\mathbb{Z}$, appelés* coefficients de Bézout, *tels que $au+bv=\mathrm{pgcd}(a,b)$. Ces coefficients ne sont pas uniques : les solutions entières de l'équation $aU+bV=d$ sont données par $\{\,(u,v)+k(\frac{b}{d},-\frac{a}{d})\mid k\in\mathbb{Z}\,\}$.*

DÉMONSTRATION. Soit d un pgcd de a et b. Comme $d|a$ et $d|b$ on a $d|au+bv$ pour tout $u,v\in\mathbb{Z}$, donc $a\mathbb{Z}+b\mathbb{Z}\subset d\mathbb{Z}$. D'autre part le sous-groupe $a\mathbb{Z}+b\mathbb{Z}$ est de la forme $c\mathbb{Z}$ pour un $c\in\mathbb{Z}$. Comme $a,b\in c\mathbb{Z}$ on a $c|a$ et $c|b$, il s'agit donc d'un diviseur commun de a et b. Pour celui-ci on sait que $c|d$, autrement dit $c\mathbb{Z}\supset d\mathbb{Z}$. On conclut que $a\mathbb{Z}+b\mathbb{Z}=d\mathbb{Z}$ comme énoncé. (Le reste est laissé en exercice.) □

Après avoir établi leur existence, il se pose la question naturelle de savoir comment trouver efficacement des coefficients de Bézout. Dans un anneau euclidien, on dispose de l'algorithme suivant :

Comme avant on construit une suite finie (r_i) commençant par $r_0=a$ et $r_1=b$ puis $r_{i+1}=r_{i-1}-r_iq_i$ par une division euclidienne itérée. Parallèlement on pose $w_0=(1,0)$ et $w_1=(0,1)$ puis $w_{i+1}=w_{i-1}-q_iw_i$. On assure ainsi que $r_i=w_i\binom{a}{b}$ pour tout i. On arrive finalement à $r_n=\mathrm{pgcd}(a,b)$ et $w_n=(u,v)$ avec $r_n=au+bv$ comme souhaité. Voici un tel algorithme « prêt à programmer » :

Algorithme IX.2 Algorithme d'Euclide-Bézout

Entrée: deux entiers a_0 et b_0

Sortie: trois entiers d,u,v tels que $d = a_0u + b_0v$ soit un pgcd de a_0 et b_0

$\begin{pmatrix} a & u & v \\ b & s & t \end{pmatrix} \leftarrow \begin{pmatrix} a_0 & 1 & 0 \\ b_0 & 0 & 1 \end{pmatrix}$ // Initialement $a = a_0u + b_0v$ et $b = a_0s + b_0t$

tant que $b \neq 0$ **faire**

division euclidienne $(q,r) \leftarrow \delta(a,b)$

$\begin{pmatrix} a & u & v \\ b & s & t \end{pmatrix} \leftarrow \begin{pmatrix} b & s & t \\ r = a - qb & u - qs & v - qt \end{pmatrix}$ // Préserve $a = a_0u + b_0v$ et $b = a_0s + b_0t$

fin tant que

si $a \geq 0$ **alors retourner** a,u,v **sinon retourner** $-a,-u,-v$ // On renvoie toujours le pgcd positif

Exercice/M 2.14. Montrer que l'algorithme IX.2 est correct. *Indication.* — Comme pour l'algorithme d'Euclide on voit que l'algorithme IX.2 s'arrête et trouve un pgcd de a_0 et b_0. Pour les coefficients de Bézout vérifier les égalités $a_k = a_0u_k + b_0v_k$ et $b_k = a_0s_k + b_0t_k$ avant et après chaque itération de la boucle.

Exercice/P 2.15. Afin d'optimiser on peut finalement remplacer le calcul itéré de v et t pendant la boucle par un seul calcul de v après la boucle. Prouver la correction de l'algorithme IX.3 ci-dessus et l'implémenter en une fonction `Integer pgcd( Integer a0, Integer b0, Integer& u, Integer& v )`.

Attention. — Les affectations « matricielles » sont une écriture commode qui ne se traduit pas littéralement : en C++ il faudra des variables auxiliaires pour ne pas écraser des valeurs dont on aura encore besoin.

Algorithme IX.3 Algorithme d'Euclide-Bézout (légèrement optimisé)

Entrée: deux entiers a_0, b_0

Sortie: trois entiers d,u,v tels que $d = a_0u + b_0v$ soit un pgcd de a_0 et b_0

$\begin{pmatrix} a & u \\ b & s \end{pmatrix} \leftarrow \begin{pmatrix} a_0 & 1 \\ b_0 & 0 \end{pmatrix}$ // Initialement $a \equiv a_0u$ et $b \equiv a_0s \pmod{b_0}$

tant que $b \neq 0$ **faire**

division euclidienne $(q,r) \leftarrow \delta(a,b)$

$\begin{pmatrix} a & u \\ b & s \end{pmatrix} \leftarrow \begin{pmatrix} b & s \\ r = a - qb & u - qs \end{pmatrix}$ // Préserve $a \equiv a_0u$ et $b \equiv a_0s \pmod{b_0}$

fin tant que

si $b_0 = 0$ **alors** $v \leftarrow 0$ **sinon** $v \leftarrow (a - a_0u)/b_0$ // On sait que b_0 divise $a - a_0u$ sans reste

si $a \geq 0$ **alors retourner** a,u,v **sinon retourner** $-a,-u,-v$ // On renvoie toujours le pgcd positif

3. Premières applications

3.1. Inversion dans l'anneau quotient $\mathbb{Z}_n$. Les anneaux quotients $\mathbb{Z}/n\mathbb{Z}$ interviennent dans nombre d'applications. On va utiliser l'écriture abrégée $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ qui est moins standard mais plus concise. (Si les algorithmiciens la trouvent bien commode, les algébristes la réservent pour un tout autre objet.)

Chaque entier a représente un élément dans $\mathbb{Z}_n$ via l'application quotient $\pi_n : \mathbb{Z} \to \mathbb{Z}_n$, $a \mapsto \pi_n(a)$. Pour les implémentations il est commode de prendre l'intervalle $[\![0,n[\![:= \{0,1,2,\ldots,n-1\}$ comme système préféré de représentants. Ainsi π_n établit une bijection entre $\{0,1,2,\ldots,n-1\}$ et $\mathbb{Z}_n$.

Exercice/M 3.1. Montrer qu'un entier a représente un élément inversible dans $\mathbb{Z}_n$ si et seulement si $\operatorname{pgcd}(a,n) = 1$. Conclure en particulier que $\mathbb{Z}_n$ est un corps si et seulement si n est premier.

Exercice/P 3.2. Écrire une fonction `Integer inverse( Integer a, Integer n )` qui renvoie l'inverse $u \in [\![1,n[\![$ de a modulo n lorsque c'est possible, et renvoie 0 sinon. Pour un traitement plus net du cas non inversible, vous pouvez implémenter, si vous préférez, deux fonctions

```
bool inversible( Integer a, Integer n )
bool inversible( Integer a, Integer n, Integer& u )
```

La première teste simplement si a est inversible modulo n, la deuxième calcule parallèlement l'inverse u de a lorsque c'est possible. *Indication.* — Dans chaque cas on pourra adapter l'algorithme IX.3 sur mesure.

3.2. Le théorème des restes chinois. Soient a et b deux entiers premiers entre eux, autrement dit $\operatorname{pgcd}(a,b)=1$. Le théorème des restes chinois affirme que pour tout $y,z\in\mathbb{Z}$ le système

$$\begin{cases} x\equiv y \pmod a \\ x\equiv z \pmod b \end{cases}$$

admet une solution $x\in\mathbb{Z}$, et que $x+\mathbb{Z}ab$ est l'ensemble de toutes les solutions. Par exemple le système $x\equiv 7 \pmod 8$ et $x\equiv 48 \pmod{125}$ admet une unique solution $x\in[\![0,1000[\![$, mais laquelle ? Évidemment il est facile de trouver y et z à partir de x, mais comment retrouver x à partir de y et z ?

Théorème 3.3 (Théorème chinois)**.** *Soit $m_1,\dots,m_k\geq 1$ une famille d'entiers et soit $m=m_1\cdots m_k$ leur produit. Alors il existe un unique homomorphisme d'anneaux $\Phi\colon \mathbb{Z}_m\to\mathbb{Z}_{m_1}\times\cdots\times\mathbb{Z}_{m_k}$, à savoir*

$$\Phi\big(\pi_m(x)\big)=\big(\pi_{m_1}(x),\dots,\pi_{m_k}(x)\big).$$

Si m_i et m_j sont premiers entre eux pour tout $i\neq j$, alors Φ est un isomorphisme. Plus explicitement, $m_i'=m/m_i=\prod_{j\neq i}m_j$ est inversible modulo m_i, il existe donc un représentant $u_i\in[\![0,m_i[\![$ de l'inverse de m_i' modulo m_i. L'application inverse de Φ est alors donnée par $\Psi\colon \mathbb{Z}_{m_1}\times\cdots\times\mathbb{Z}_{m_k}\to\mathbb{Z}_m$

$$\Psi\big(\pi_{m_1}(y_1),\dots,\pi_{m_1}(y_k)\big)=\pi_m\big(y_1u_1m_1'+\cdots+y_ku_km_k'\big).$$

Attention. — Si les entiers $m_1,\dots,m_k$ ne sont pas premiers entre eux, alors l'homomorphisme Φ existe toujours mais il n'est plus un isomorphisme. Le détailler pour $\Phi\colon\mathbb{Z}_4\to\mathbb{Z}_2\times\mathbb{Z}_2$ en explicitant image et noyau. Montrer plus généralement qu'il n'existe pas d'homomorphisme de groupes entre $\mathbb{Z}_4$ et $\mathbb{Z}_2\times\mathbb{Z}_2$.

Exercice/M 3.4. Prouver le théorème : montrer que Φ est bien définie (existence) et qu'ici c'est le seul homomorphisme d'anneaux possible (unicité). Les formules pour Φ et Ψ sont explicites ; on peut donc calculer directement $\Psi\circ\Phi$ et $\Phi\circ\Psi$ pour montrer que ces applications sont inverses l'une à l'autre.

Exemple 3.5. Appliquons le théorème pour résoudre le système suivant :

$$\begin{cases} x &\equiv& 18000 & \pmod{19687} \\ x &\equiv& 13 & \pmod{17} \end{cases}$$

Avec $a=19687$ et $b=17$ on trouve $\operatorname{pgcd}(a,b)=1$ avec des coefficients de Bézout $u=1$ et $v=-1158$. On a $ab=334679$ et $bv=-19686$ et $au=19687$, et ainsi l'application inverse cherchée est ici

$$\Psi(\pi_a(y),\pi_b(z))=\pi_{ab}(-19686y+19687z).$$

Pour $y=18000$ et $z=13$ on trouve la solution $x=-354092069$. On réduit ensuite ce nombre modulo ab, ce qui donne $x=332992$. Vous pouvez finalement vérifier que $x\equiv y \pmod a$ et $x\equiv z \pmod b$.

À noter que malgré la petitesse du nombre cherché $x\in[\![0,ab[\![$ le calcul provoque l'apparition d'une quantité mille fois plus grande. Ce phénomène est assez général et montre que la formule explicitée dans le théorème n'est pas optimale pour le calcul : une implémentation maladroite de l'application Ψ peut largement dépasser l'intervalle $[\![0,m[\![$. Soulignons donc que *l'application* Ψ est unique, mais la *formule explicite* pour son calcul ne l'est pas ! Il convient donc d'en développer une autre qui soit plus efficace.

3.3. Un développement plus efficace. Nous donnons ici une démonstration alternative du théorème chinois qui reprend l'idée de numération en base mixte. Cette approche a le mérite de produire une formule plus efficace. Rappelons que tout entier $x\in[\![0,m_1m_2\cdots m_k[\![$ s'écrit de manière unique comme

$$x=x_1+m_1x_2+m_1m_2x_3+\cdots+m_1m_2\cdots m_{k-1}x_k$$

avec des « chiffres » $x_i\in[\![0,m_i[\![$. Ceci n'est rien autre que la numération dans la base mixte donnée par les « poids » $m_1,m_2,\dots,m_k$. (Voir le chapitre II et l'annexe II.)

Comment trouver x tel que $x\equiv y_1 \pmod{m_1}$? Évidemment il faut poser $x_1=y_1 \bmod m_1$. Comment satisfaire en plus à $x\equiv y_2 \pmod{m_2}$? Ici il suffit de résoudre $x_1+m_1x_2\equiv y_2 \pmod{m_2}$, posons donc $x_2=[u_2(y_2-x_1)] \bmod m_2$, où l'entier $u_2\in[\![0,m_2[\![$ représente l'inverse de m_1 modulo m_2. On peut ainsi continuer à calculer un par un les coefficients $x_1,x_2,\dots,x_n$:

Théorème 3.6. *Soit $m_1,\dots,m_k \geq 1$ une famille d'entiers, premiers entre eux deux à deux. Soit $u_k \in [\![0,m_k[\![$ l'inverse de $m_1\dots m_{k-1}$ modulo m_k. Étant donné $y_1,\dots,y_k \in \mathbb{Z}$ l'algorithme suivant calcule l'unique entier $x = a_k \in [\![0,m_1\cdots m_k[\![$ de sorte que $x \equiv y_1 \pmod{m_1}$, …, $x \equiv y_k \pmod{m_k}$:*

$$\begin{aligned}
&x_1 \leftarrow y_1 \bmod m_1 && a_1 \leftarrow x_1\\
&x_2 \leftarrow [u_2(y_2-a_1)] \bmod m_2 && a_2 \leftarrow a_1 + m_1x_2\\
&x_3 \leftarrow [u_3(y_3-a_2)] \bmod m_3 && a_3 \leftarrow a_2 + m_1m_2x_3\\
&\vdots\\
&x_k \leftarrow [u_k(y_k-a_{k-1})] \bmod m_k && a_k \leftarrow a_{k-1} + m_1\cdots m_{k-1}x_k
\end{aligned}$$

De plus, cet algorithme est le plus économe possible dans le sens que tous les calculs intermédiaires se placent dans l'intervalle $[\![0,m_1\cdots m_k[\![$.

Exercice/M 3.7. Prouver ce théorème. Vérifier que $x_i \in [\![0,m_i[\![$ et que $a_i \in [\![0,m_1\cdots m_i[\![$ par construction. Il ne reste qu'à montrer les congruences souhaitées $a_i \equiv y_j \pmod{m_j}$ pour $j \leq i$.

Exemple 3.8. Reprenons l'exemple précédent avec $a = 19687$, $b = 17$, donc $u = 1$. Pour $y = 18000$ et $z = 13$ on calcule $r = u(z-y) \bmod b = 16$, puis $x = y + ar = 332992$, ce qui est bien le nombre cherché.

Exemple 3.9. Pour son examen oral un étudiant X doit réunir deux examinateurs : Le professeur A ne peut que tous les 12 jours à partir de lundi, 1er janvier. Le professeur B ne peut que les mercredis. Quelles sont les dates possibles ? (Vous pouvez trouver la solution sans aucune théorie, bien sûr. Il sera néanmoins instructif de comparer votre solution avec les formules ci-dessus en précisant les étapes du calcul.)

Remarque 3.10. Ce genre de calcul permettait aux généraux chinois de dénombrer leur troupe, sans trop d'efforts pour eux-mêmes, en ordonnant : « rangez-vous 7 par 7, puis 11 par 11, puis 13 par 13, puis 17 par 17 ». Si cette anecdote est vraie on peut en déduire une borne maximum du nombre des soldats dans une troupe, et une grande agitation pendant le dénombrement.

Exercice/P 3.11. Écrire un programme qui lit un par un les couples $(m_1,y_1),\dots,(m_k,y_k)$. Il s'arrête si l'utilisateur entre la valeur $m_k = 0$ ou bien si $m_1,m_2,\dots,m_k$ ne sont plus premiers entre eux. Autrement il affiche l'unique solution $x \in [\![0,m_1m_2\cdots m_k[\![$ vérifiant les congruences $x \equiv y_i \pmod{m_i}$ pour tout $i \leq k$, puis continue à demander (m_{k+1},y_{k+1}).

Exercice 3.12. Une fermière va au marché avec une charrette plein d'oeufs. Le ministre de l'agriculture (plus exactement son chauffeur) brûle un feu rouge et casse tous les oeufs. Bien sûr un fond de l'Union Européenne est prévu précisément pour de tels accidents. Malheureusement la fermière, traumatisée par le choc, se souvient seulement qu'elle avait essayé de ranger ses oeufs par $2,3,4,5,6$ et chaque fois il en restait un, et qu'elle avait pu finalement les ranger par 7. Le ministre suppose qu'elle avait moins de 600 oeufs, ce qui est le plafond exigé par l'administration (dont on ignore les raisons). Les intéressés arrivent-ils à remplir les formulaires nécessaires ? La fermière combien d'oeufs avait-elle ? Quel est l'âge du chauffeur ?

Une astuce qui sert plus qu'une fois est une théorie.
anonyme

COMPLÉMENT IX

Le vocabulaire des anneaux

Le bref résumé qui suit est une invitation à relire votre cours d'algèbre. Pour notre propos l'exemple phare est l'anneau $\mathbb{Z}$ des entiers et l'algorithme d'Euclide. Avant tout nous essayerons donc d'approfondir la notion d'anneau euclidien introduite en §1.2 au début de ce chapitre. En même temps il semble utile de rappeler les notions de base afin de fixer le vocabulaire des anneaux commutatifs, surtout de la trilogie des anneaux *euclidiens, principaux, factoriels*. Ceci servira à mieux situer le cas particulier $\mathbb{Z}$ et de préparer de futures implémentations d'anneaux plus généraux.

Sommaire

1. Anneaux et corps

1.1. Anneaux. Commençons par le tout début (ou presque) :

Définition 1.1. Un *anneau* $(A,+,\cdot)$ est un ensemble A muni de deux applications, *l'addition* $+\colon A\times A\to A$ et la *multiplication* $\cdot\colon A\times A\to A$, de sorte que $(A,+)$ soit un groupe abélien, que $(A,\cdot)$ soit un monoïde, et que la multiplication soit distributive sur l'addition. La distributivité veut dire que pour tout $x,y,z\in A$ on a

$$x\cdot(y+z)=(x\cdot y)+(x\cdot z),$$
$$(x+y)\cdot z=(x\cdot z)+(y\cdot z).$$

On note $0=0_A$ l'élément neutre pour l'addition et $1=1_A$ l'élément neutre pour la multiplication ; ils sont uniquement déterminés par la structure d'anneau. On exige que $1\neq 0$ pour exclure le cas dégénéré $A=\{0\}$.

Remarque 1.2. La distributivité implique pour tout $a\in A$ que $a\cdot 0=a\cdot(0+0)=a\cdot 0+a\cdot 0$ donc $a\cdot 0=0$. De la même manière $a\cdot(-1)+a=a\cdot(-1)+a\cdot 1=a(-1+1)=a\cdot 0=0$ donc $a\cdot(-1)=-a$. De même $0\cdot a=0$ et $(-1)\cdot a=-a$.

Définition 1.3. Un anneau $(A,+,\cdot)$ est dit *commutatif* si la multiplication $\cdot$ est commutative.

Sauf mention du contraire nous supposerons dans la suite que les anneaux considérés sont commutatifs.

Exemple 1.4. Voici quelques exemples d'anneaux : l'anneau des entiers, noté $\mathbb{Z}$; les entiers modulo n, noté $\mathbb{Z}_n$; les nombres rationnels $\mathbb{Q}$, réels $\mathbb{R}$, complexes $\mathbb{C}$, tous avec leurs opérations usuelles. Les nombres naturels $\mathbb{N}$ avec leur addition et leur multiplication usuelles ne forment pas un anneau car $(\mathbb{N},+)$ n'est pas un groupe.

Exemple 1.5. Si $(A_i)_{i\in I}$ est une famille d'anneaux, alors leur produit cartésien $A=\prod_{i\in I}A_i$ est un anneau pour l'addition $(a_i)_{i\in I}+(b_i)_{i\in I}=(a_i+b_i)_{i\in I}$ et la multiplication $(a_i)_{i\in I}\cdot(b_i)_{i\in I}=(a_i\cdot b_i)_{i\in I}$. Dans le cas d'une famille finie d'anneaux $A_1,\dots,A_n$ on écrit aussi $A=A_1\times\cdots\times A_n$ pour leur produit cartésien.

Exemple 1.6. Si A est un anneau, on peut construire l'anneau $A[X]$ des polynômes en une variable X à coefficients dans A. (Le chapitre XIII présentera un développement détaillé.) Cette construction peut être itérée : $A[X,Y]=A[X][Y]$ est l'anneau des polynômes en deux variables, $A[X,Y,Z]=A[X,Y][Z]$ est l'anneau des polynômes en trois variables, etc.

Définition 1.7. Un *sous-anneau* d'un anneau $(A,+,\cdot)$ est une partie $B\subset A$ telle que $(B,+)$ soit un sous-groupe de $(A,+)$ ainsi qui $(B,\cdot)$ soit un sous-monoïde de $(A,\cdot)$. Dans ce cas $(B,+,\cdot)$ est un anneau pour la restriction de l'addition et de la multiplication.

Remarque 1.8. Si $(B_i)_{i\in I}$ est une famille de sous-anneaux d'un anneau A, alors l'intersection $B=\bigcap_{i\in I}B_i$ est un sous-anneau de A. *Attention.* — La réunion de sous-anneaux n'est en général pas un sous-anneau.

Définition 1.9. Soient A un anneau, $B\subset A$ un sous-anneau et $S\subset A$ une partie quelconque. On note $B[S]$ le plus petit sous-anneau de A contenant B et S, appelé *anneau engendré* par S sur B.

Exemple 1.10. Dans $\mathbb{C}$ on note $\mathbb{Z}[i]$ l'anneau engendré par i sur $\mathbb{Z}$. Montrer que $\mathbb{Z}[i]=\{a+bi \mid a,b\in\mathbb{Z}\}$.

Exemple 1.11. Dans $\mathbb{R}$ on note $\mathbb{Q}[\sqrt{2}]$ l'anneau engendré par $\sqrt{2}$ sur $\mathbb{Q}$. Montrer que $\mathbb{Q}[\sqrt{2}]=\{a+b\sqrt{2} \mid a,b\in\mathbb{Q}\}$.

Très souvent on veut conclure que $ab=0$ implique $a=0$ ou $b=0$. Cette propriété ne fait pas partie de la définition d'anneau, et elle n'est pas vérifié dans $\mathbb{Z}_6$, par exemple.

Définition 1.12. On note $A^*=A\smallsetminus\{0\}$ l'ensemble des éléments non nuls. Un élément $a\in A^*$ est un *diviseur de zéro* s'il existe $b\in A^*$ tel que $ab=0$. L'anneau A est *intègre* s'il n'admet pas de diviseurs de zéro, c'est-à-dire si $ab=0$ implique $a=0$ ou $b=0$. Autrement dit, A est intègre si $(A^*,\cdot)$ est un monoïde.

Exemple 1.13. L'anneau $\mathbb{Z}$ est intègre. L'anneau $\mathbb{Z}_n$ est intègre si et seulement si n est premier.

Exemple 1.14. Dans un anneau intègre tout sous-anneau est intègre. En particulier $\mathbb{Z}[i]\subset\mathbb{C}$ est intègre.

Exemple 1.15. Un anneau produit $A=A_1\times\cdots\times A_n$ avec $n\geq 2$ n'est jamais intègre. (Pourquoi ?)

Définition 1.16. Un élément $u\in A$ est dit *inversible* s'il existe $v\in A$ de sorte que $uv=1$. On note $A^\times$ le groupe multiplicatif des éléments inversibles dans A. On dit que A est un *corps* si $A^\times=A^*$, c'est-à-dire si tout élément non nul admet un inverse. Autrement dit, A est un corps si $(A^*,\cdot)$ est un groupe.

Exemple 1.17. Bien sûr $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps, et $\mathbb{Z}$ ne l'est pas : $\mathbb{Z}^\times=\{\pm1\}$ diffère de $\mathbb{Z}^*=\mathbb{Z}\smallsetminus\{0\}$. Les éléments de $\mathbb{Z}_n^\times$ correspondent aux entiers qui sont premiers avec n, et $\mathbb{Z}_n$ est un corps ssi n est premier.

Exercice 1.18. Un anneau intègre fini A est un corps. *Indication.* — Pour $a\in A^*$ la multiplication $x\mapsto ax$ définit une application $\gamma_a\colon A\to A$. Montrer qu'elle est injective, puis bijective. Conclure.

Définition 1.19. Le groupe $A^\times$ agit naturellement sur A via la restriction $A^\times\times A\to A$ de la multiplication. Deux éléments $a,b\in A$ sont *associés*, noté $a\sim b$, s'ils sont dans la même orbite sous cette action, c'est-à-dire s'il existe $u\in A^\times$ tel que $ua=b$. (Vérifier qu'il s'agit d'une relation d'équivalence.)

Exemple 1.20. Dans $\mathbb{Z}$ on a $\mathbb{Z}^\times=\{\pm1\}$, donc a et $-a$ sont associés. Dans chaque classe d'éléments associés on distingue ici un élément préféré : l'unique élément non négatif. Par exemple, pour calculer le pgcd de deux nombres entiers, on préfère le pgcd positif. Pour le moment ceci n'est qu'une convention pour rendre le pgcd unique.

Exercice 1.21. Si $a\sim b$ alors $a\mid b$ et $b\mid a$. Dans un anneau intègre on a aussi la conclusion réciproque.

1.2. Divisibilité. Bien connue des entiers, la notion de divisibilité se retrouve naturellement dans la théorie des anneaux :

Définition 1.22. On dit que *a divise b* dans A, noté $a\mid b$, s'il existe $c\in A$ de sorte que $ac=b$. On dit que c est un diviseur commun de $x_1,\dots,x_n$ dans A si $c\mid x_i$ pour tout i. On dit que d est un *plus grand commun diviseur* de $x_1,\dots,x_n$ s'il est un diviseur commun et que tout autre diviseur commun c divise aussi d.

Exercice 1.23. La divisibilité $a\mid b$ définit un ordre partiel sur A, dont 1 est un plus petit élément et 0 est le plus grand élément (le vérifier). Les éléments inversibles sont exactement les diviseurs de 1. Dans un anneau intègre $a\mid b$ et $b\mid a$ entraîne $a\sim b$ (le vérifier). Dans ce cas les pgcd de $x_1,\dots,x_n$ sont associés entre eux.

On connaît les notions *irréductible* et *premier* de l'anneau $\mathbb{Z}$, où elles coïncident. Pour un anneau général il faut les distinguer par une définition précise :

Définition 1.24. Un élément $a\in A$ est *irréductible* si $a=bc$ entraîne ou $b\in A^\times$ ou $c\in A^\times$.

Définition 1.25. Un élément $p\in A$ est *premier* s'il n'est pas inversible et si $p\mid ab$ entraîne $p\mid a$ ou $p\mid b$.

Exercice 1.26. Par définition un élément irréductible n'est ni nul ni inversible. (Relire la définition.) Par contre, l'élément 0 peut être premier (expliciter sous quelle condition exactement). L'irréductibilité de a veut dire que a n'admet pas de facteurs non triviaux : si $b\mid a$, alors $b\sim 1$ ou $b\sim a$. Montrer qu'un élément premier non nul est irréductible. (La réciproque est fausse en générale, voir l'exercice 4.6.)

1.3. Homomorphismes. Comme pour tout objet algébrique, la notion d'homomorphisme est primordiale pour la théorie des anneaux.

Définition 1.27. Un *homomorphisme* entre deux anneaux unitaires A et A' est une application $\varphi\colon A \to A'$ vérifiant $\varphi(a+b) = \varphi(a)+\varphi(b)$ pour tout $a,b \in A$, ainsi que $\varphi(a\cdot b) = \varphi(a)\cdot\varphi(b)$ et $\varphi(1) = 1$.

Exemple 1.28. Pour tout anneau A l'identité id_A est un homomorphisme. Si $f\colon A \to B$ et $g\colon B \to C$ sont des homomorphismes d'anneaux, alors leur composée $g\circ f\colon A \to C$ est un homomorphisme d'anneaux.

Remarque 1.29. Si $B \subset A$ est un sous-anneau, alors l'inclusion $B \hookrightarrow A$ est un homomorphisme d'anneaux.

Remarque 1.30. Soit $\varphi\colon A \to A'$ un homomorphisme d'anneaux. Alors pour tout sous-anneau B de A, l'image $\phi(B)$ est un sous-anneau de A'. Pour tout sous-anneau B' de A', l'image réciproque $\phi^{-1}(B')$ est un sous-anneau de A.

Définition 1.31. Un *isomorphisme* d'anneaux est un homomorphisme bijectif.

Remarque 1.32. Un homomorphisme d'anneaux $\varphi\colon A \to A'$ est un isomorphisme si et seulement s'il existe un homomorphisme d'anneaux $\psi\colon A' \to A$ tel que $\psi\circ\varphi = \mathrm{id}_A$ et $\varphi\circ\psi = \mathrm{id}_{A'}$. (Le montrer.)

Exemple 1.33. La projection canonique $\mathbb{Z} \to \mathbb{Z}_n$ est un homomorphisme surjectif mais non injectif (pourvu que *nne*0). L'inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$ est un homomorphisme injectif mais non surjectif.

Exemple 1.34. Pour toute paire $m,n \in \mathbb{Z}$ il existe un unique homomorphisme d'anneaux $\varphi\colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$. C'est un isomorphisme si et seulement si m et n sont premiers entre eux. (Le montrer.) Dans ce cas on obtient un isomorphisme des groupes multiplicatifs $\varphi^\times\colon \mathbb{Z}_{mn}^\times \to \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$.

1.4. Idéaux. Après les homomorphismes il est naturel de regarder les idéaux :

Définition 1.35. Pour un sous-ensemble $I \subset A$ on définit $AI := \{ax \mid a \in A, x \in I\}$. Un *idéal* I est un sous-groupe additif de A tel que $AI = I$, c'est-à-dire pour tout $a \in A$ et $x \in I$ on a $ax \in I$.

Exemple 1.36. Pour $x \in A$ l'ensemble $(x) = Ax = \{ax \mid a \in A\}$ est un idéal, dit l'idéal *principal* engendré par x. Plus généralement toute famille $x_1,\dots,x_n \in A$ engendrent un idéal $(x_1,\dots,x_n) := \{a_1x_1 + \cdots + a_nx_n \mid a_i \in A\}$, et tout sous-ensemble $X \subset A$ engendre un idéal $(X) := \{\sum a_ix_i \mid a_i \in A, x_i \in X\}$. (Vérifier qu'il s'agit d'idéaux.)

Exemple 1.37. L'idéal (0) est réduit à l'élément 0. L'idéal (1) est l'anneau A tout entier. Il se peut que ce soient les seuls : A est un corps si et seulement si (0) et (1) sont les seuls idéaux dans A (le montrer).

Exercice 1.38. Toute question de divisibilité se reformule en terme d'idéaux. Vérifier par exemple que $a \mid b$ équivaut à $(b) \subset (a)$. Ensuite montrer que d est un pgcd de $x_1,\dots,x_n$ si et seulement si (d) est le plus petit idéal principal qui contienne $(x_1,\dots,x_n)$. Formuler puis montrer un énoncé analogue pour le ppcm.

Proposition 1.39. *Pour un homomorphisme $\varphi\colon A \to A'$ on note* $\ker(\varphi) := \{a \in A \mid \varphi(a) = 0\}$ *son* noyau. *Il s'agit d'un idéal de A. Réciproquement tout idéal I de A donne lieu à un anneau quotient A/I tel que la projection canonique $\pi\colon A \to A/I$ soit un homomorphisme d'anneaux avec* $\ker(\pi) = I$.

Exercice 1.40. Soit A un anneau et $I \subset A$ un idéal. Alors la projection canonique $\pi\colon A \to A/I$ établit une bijection entre les idéaux J contenant I et les idéaux de l'anneau quotient A/I, définie par $J \mapsto J/I$. Montrer ainsi que les idéaux de l'anneau $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ sont de la forme $n\mathbb{Z}/m\mathbb{Z}$ où $n \mod m$. Expliciter le treilli des idéaux de $\mathbb{Z}_{12}$.

Définition 1.41. Un idéal $I \subset A$ est dit *premier* si A/I est intègre, et *maximal* si A/I est un corps.

Remarque 1.42. Autrement dit, un idéal $I \subset A$ est premier si et seulement $I \neq A$ et $ab \in I$ implique $a \in I$ ou $b \in I$.

Si A/I est un corps, alors en particulier A/I est intègre, donc tout idéal maximal $I \subset A$ est premier.

Si A/I est un corps alors ses seuls idéaux sont 0 et A/I. Les seuls idéaux de A contenant I sont donc I et A. Ceci implique que I est maximal si et seulement si tout idéal J vérifiant $I \subset J \subset A$ est soit $J = I$ soit $J = A$.

Théorème 1.43. *Tout homomorphisme $\varphi\colon A \to A'$ factorise de manière unique comme $\varphi = \iota\bar{\varphi}\pi$ par la projection $\pi\colon A \to A/\ker(\varphi)$, un isomorphisme $\bar{\varphi}\colon A/\ker(\varphi) \to \mathrm{im}(\varphi)$, et l'inclusion $\iota\colon \mathrm{im}(\varphi) \to A'$.*

Exemple 1.44. Tout anneau A admet un unique homomorphisme $\varphi\colon \mathbb{Z} \to A$. (Le construire.) Son image est le plus petit sous-anneau de A. (Pourquoi ?) Son noyau $\ker(\varphi) = (n)$ est engendré par un certain entier $n \geq 0$. On appelle n la *caractéristique* de l'anneau A. Ainsi tout anneau de caractéristique n contient donc un sous-anneau isomorphe à $\mathbb{Z}_n$.

2. Anneaux euclidiens

2.1. Stathmes euclidiens. Les notions de division euclidienne et de stathme euclidien on été précisées dans la définition 1.1 du chapitre IX. Pour un stathme donné $\nu\colon A\to\mathbb{N}$ il existe en général plusieurs divisions euclidiennes possibles ; pour une implémentation il faut donc spécifier laquelle on choisit.

Exercice 2.1. Soit $\nu\colon A\to\mathbb{N}$ un stathme euclidien ; on fixe deux applications $\operatorname{div},\operatorname{mod}\colon A\times A^*\to A$ de sorte que le quotient $q=a\operatorname{div}b$ et le reste $r=a\bmod b$ satisfassent $a=bq+r$ et $\nu(r)<\nu(b)$. Bien que commode, la donnée de deux applications div et mod est un peu redondante : expliquer comment définir mod à partir de div, et réciproquement comment définir div à partir de mod (dans un anneau intègre).

Exercice 2.2. Dans ce cours nous considérons des stathmes euclidiens à valeurs dans $\mathbb{N}$. Après réflexion, on n'utilise que l'ordre sur $\mathbb{N}$. Essayons donc de dégager les propriétés nécessaires pour l'algorithme d'Euclide :

Soit N un ensemble muni d'une relation d'ordre $\leq$ tel que toute partie non vide $S\subset N$ admette un plus petit élément. Dans ce cas on dit que $(N,\leq)$ est un *ensemble bien ordonné*. Montrer que toute suite décroissante $n_1>n_2>n_3>\dots$ dans N est forcément de longueur finie. Définir ce qui est un anneau euclidien avec stathme $\nu\colon A\to N$. Vérifier que l'algorithme d'Euclide reste correct dans ce cadre généralisé. Pour un exemple non trivial, regarder l'anneau $A=\mathbb{Z}\times\mathbb{Z}$ avec le stathme $\nu\colon A\to\mathbb{N}^2$, $\nu(a,b)=(|a|,|b|)$. Ici il convient de munir $\mathbb{N}^2$ de l'ordre lexicographique. Vérifier que A admet une division euclidienne par rapport à ν. (Avouons que A est facile à construire mais il n'est pas intègre, il n'est donc pas euclidien dans le sens de la définition usuelle. Il existe aussi de tels exemples intègres.)

2.2. Le stathme minimal. Si A est euclidien, le stathme $\nu\colon A\to\mathbb{N}$ n'est pas unique : par exemple on peut le composer avec une application $\phi\colon\mathbb{N}\to\mathbb{N}$, $\phi(0)=0$, ϕ strictement croissante. Par contre on peut s'intéresser au plus petit stathme euclidien sur A.

Exercice 2.3. Soit A un anneau euclidien. On définit $\mu\colon A\to\mathbb{N}$ par $\mu(x)=\min_\nu\nu(x)$ où ν parcourt tous les stathmes euclidiens sur A. Montrer que μ est un stathme euclidien.

Exercice 2.4. Un corps K est-il un anneau euclidien ? Est-ce que toute fonction $\nu\colon K\to\mathbb{N}$, avec $\nu(a)=0$ ssi $a=0$, est un stathme euclidien ? Quelle est donc le plus petit stathme euclidien sur K ? Réciproquement, un anneau avec un stathme euclidien qui ne prend que deux valeurs, est-il un corps ?

Exercice 2.5. Même pour $\mathbb{Z}$ la valeur absolue $a\mapsto|a|$ n'est pas le seul stathme intéressant. Rappelons que $\operatorname{len}\colon\mathbb{Z}\to\mathbb{N}$ associe à chaque entier a la longueur de son développement binaire, c'est-à-dire $\operatorname{len}a:=\min\{\ell\in\mathbb{N}\mid|a|<2^\ell\}$, donc $\operatorname{len}0=0$ et $\operatorname{len}(a)=1+\lfloor\log_2|a|\rfloor$ pour $a\neq0$. Montrer que len est un stathme euclidien sur $\mathbb{Z}$: pour tout a et $b\neq0$ dans $\mathbb{Z}$ il existe $q,r\in\mathbb{Z}$ tels que $a=bq+r$ et $\operatorname{len}(r)<\operatorname{len}(b)$. Prouver qu'il s'agit même du stathme minimal.

Exercice 2.6. Le stathme euclidien minimal est canonique dans le sens qu'il ne dépend que de la structure d'anneau. Soit A un anneau intègre. On définit une famille croissante $A_0\subset A_1\subset A_2\subset\dots\subset A$ comme suit. On pose $A_0=\{0\}$ puis par récurrence $A_n=A_{n-1}\cup\{a\in A\mid aA+A_{n-1}=A\}$. On constate par exemple que $A_1=\{0\}\cup A^\times$. Montrer que A est euclidien si et seulement si $A=\bigcup A_n$; dans ce cas la fonction $\mu\colon A\to\mathbb{N}$ définie par $\mu(a)=\min\{n\in\mathbb{N}\mid a\in A_n\}$ est le stathme euclidien minimal sur A.

Exercice 2.7. Outre son intérêt théorique, le stathme euclidien minimal assure un fonctionnement efficace de l'algorithme d'Euclide ; il évite en particulier la pathologie rencontrée dans l'exercice 2.8 du chapitre IX. Montrer que le stathme euclidien minimal μ a d'autres propriétés sympathiques :

(1) On a $\mu(a)=1$ si et seulement si a est inversible. Si $\mu(a)=2$ alors a est irréductible.

(2) Pour tout $a,b\in A^*$ on a $\mu(ab)\geq\mu(a)$, avec égalité si et seulement si b est inversible. (facile)

(3) Pour tout $a,b\in A^*$ on a même $\mu(ab)\geq\mu(a)+\mu(b)-1$. (plus fort mais plus difficile)

(4) Soit δ une division euclidienne par rapport au stathme μ. Si $a=bq$ alors $\delta(a,b)=(q,0)$.

Rappeler que ce sont des propriétés bien connues des stathmes euclidiens « raisonnables » sur $\mathbb{Z}$.

Exercice 2.8. On rappelle que $b\mapsto|b|$ est un stathme euclidien sur $\mathbb{Z}$. À titre d'avertissement regardons $\nu\colon\mathbb{Z}\to\mathbb{N}$ définie par $\nu(b)=b$ si $b\geq0$, et $\nu(b)=-2b$ si $b<0$. Montrer que c'est un stathme euclidien, mais aucune des propriétés sympathiques énoncées dans l'exercice précédent n'est vérifiée. Ceci souligne que nous avons tout intérêt d'utiliser le stathme minimal, ou au moins d'exiger certaines de ses propriétés.

Pour une discussion approfondie d'anneaux euclidiens, et des solutions aux exercices précédents, nous renvoyons à l'article de P. Samuel, *About Euclidean Rings*, Journal of Algebra 19 (1971), pages 282–301, dont le §4 traite du stathme euclidien minimal.

3. Anneaux principaux

3.1. Motivation. Étant donnée une famille d'éléments $a_1,\dots,a_n \in A$ et $b \in A$ on considère l'équation $a_1x_1+\cdots+a_nx_n = b$. On veut savoir si elle admet une solution $(x_1,\dots,x_n) \in A^n$ et on souhaite en trouver une le cas échéant. Plus généralement on voudrait décrire toutes les solutions en terme d'une solution particulière et une famille engendrant toutes les solutions du problème homogène $a_1x_1+\cdots+a_nx_n = 0$.

Remarque 3.1. Supposons que notre anneau A admet une solution algorithmique à ce problème. Dans ce cas on peut en particulier déterminer si b appartient à l'idéal $(a_1,\dots,a_n)$. On peut ainsi déterminer : si a est inversible dans A, ce qui équivaut à $1 \in (a)$; si a est divisible par b dans A, ce qui équivaut à $a \in (b)$; si a,b sont associés dans A, ce qui équivaut à $(a) = (b)$, c'est-à-dire $a \in (b)$ et $b \in (a)$. La liste des applications est longue…

Un cadre adéquat pour traiter les équations linéaires sont les anneaux principaux :

Définition 3.2. Un idéal $I \subset A$ est *principal* s'il est engendré par un seul élément, c'est-à-dire que $I = (a)$ pour un certain $a \in I$. Un anneau A est dit *principal* s'il est intègre et tout idéal I dans A est principal.

Exercice 3.3. On a vu que l'anneau $\mathbb{Z}$ est principal. L'anneau $\mathbb{Z}[X]$ des polynômes sur $\mathbb{Z}$, par contre, n'est pas principal : l'idéal $(2,X)$ par exemple n'est pas principal.

Exercice 3.4. Vérifier que dans un anneau principal d est un pgcd de $x_1,\dots,x_n$ si et seulement si $(d) = (x_1,\dots,x_n)$. En déduire une identité de Bézout. Si l'anneau n'est pas principal, la situation se complique : Dans $\mathbb{Z}[X]$, montrer que 1 est un pgcd de 2 et X, mais $(1) \subsetneq (2,X)$. Dans un tel cas il est inutile de chercher des coefficients de Bézout.

Exercice 3.5. Montrer que tout anneau euclidien est principal, en s'inspirant de la preuve que nous avons vue pour $\mathbb{Z}$.

Remarque 3.6. Légèrement plus généraux que les anneaux euclidiens, les anneaux principaux forment une classe plus grande mais encore bien maniable. Il existe des anneaux principaux non euclidiens, par exemple le fameux anneau $\mathbb{Z}[\sqrt{-19}]$, mais une analyse détaillée nous entraînerait trop loin.

3.2. Aspects algorithmiques. Comme dans le cas euclidien, une implémentation d'un anneau principal nécessitera une fonction concrète pour les coefficients de Bézout. Voici une formulation précise :

Définition 3.7. Soit A un anneau. Une *fonction de Bézout* est une application $\beta : A\times A \to A\times A$, $(a,b) \mapsto (u,v)$ telle que $au+bv$ soit un pgcd de a et b.

Remarque 3.8. Sur un anneau principal il existe toujours des fonctions de Bézout. Comme on a vu dans le cas $\mathbb{Z}$, il est illusoire d'espérer unicité ; le mieux que l'on puisse faire est d'en choisir une selon le contexte. Après l'existence, le vrai problème est le calcul efficace : étant donné (a,b) dans un anneau principal, comment trouver des coefficients de Bézout ? Heureusement cette difficulté disparaît dans le cas euclidien :

Exercice 3.9. Si A est euclidien, montrer que l'algorithme d'Euclide étendu définit une fonction de Bézout.

Exercice 3.10. Étant donné une fonction de Bézout sur A, montrer que tout idéal finiment engendré de A est principal. (A priori il peut y avoir de méchants idéaux qui ne sont pas finiment engendrés, et donc non principaux. On exclut cette pathologie en exigeant que A soit *noethérien*.)

Exercice 3.11. L'équation $a_1x_1+\cdots+a_nx_n = b$ admet une solution si et seulement si l'idéal $(a_1,\dots,a_n)$ contient l'élément b. Pour $n = 1$ il s'agit de tester la divisibilité de b par a_1 ; calculer la solution x_1 revient à diviser b par a_1. Pour $n = 2$, supposons que A est principal avec fonction de Bézout β. Expliciter un algorithme pour résoudre l'équation $a_1x_1+a_2x_2 = b$. Esquisser un solution du problème général $a_1x_1+\cdots+a_nx_n = b$ (par récurrence).

Remarque 3.12. Le traitement algorithmique d'idéaux dans $\mathbb{Z}[X]$ et $K[X,Y]$, voire dans $K[X_1,\dots,X_n]$, est un problème assez profond, et hors de la portée de ce cours. Il en existe une solution via les *bases de Gröbner* et les algorithmes associés. Si cela vous intéresse, lisez le premier chapitre de *Some Tapas of Computer Algebra* édité par A.M. Cohen, H. Cuypers et H. Sterk (Springer-Verlag, Berlin 1999).

Exercice 3.13. Dans tout anneau A on a les équivalences : a est premier $\Leftrightarrow$ l'idéal (a) est premier $\Leftrightarrow$ $A/(a)$ est intègre. Dans $\mathbb{Z}$ par exemple n est premier ssi $\mathbb{Z}/(n)$ est intègre. Dans ce cas $\mathbb{Z}/(n)$ est même un corps (rappeler pourquoi). On conclut que (n) est même un idéal maximal. Ce phénomène n'est pas un hasard :

Exercice 3.14. Pour un élément $a \neq 0$ d'un anneau principal A sont équivalents : l'élément a est irréductible $\Leftrightarrow$ l'idéal (a) est premier $\Leftrightarrow$ l'idéal (a) est maximal. Expliquer en rétrospective pourquoi dans $\mathbb{Z}$ on ne voit pas certaines subtilités, qui risquent de se produire dans des anneaux plus généraux.

4. Anneaux factoriels

4.1. Factorisation. Au début du chapitre on a mentionné la structure factorielle de l'anneau $\mathbb{Z}$. Dans un cours d'algèbre on en extrait l'abstraction suivante. Étant donné une partie $P \subset A$ on note $\mathbb{N}^{(P)}$ l'ensemble des fonctions $\nu\colon P \to \mathbb{N}$ à support fini, c'est-à-dire que $\nu_p = 0$ pour tout $p \in P$ sauf un nombre fini. Cette précaution permet de définir l'application $\Pi_P\colon A^\times \times \mathbb{N}^{(P)} \to A^*$ par $\Pi_P(u,\nu) = u \cdot \prod_{p\in P} p^{\nu_p}$. À noter qu'il s'agit bien d'un produit *fini*, bien que l'ensemble P puisse être infini.

Définition 4.1. Une *structure factorielle* sur un anneau A est une partie $P \subset A$ telle que l'application $\Pi_P\colon A^\times \times \mathbb{N}^{(P)} \to A^*$ soit une bijection. Dans ce cas l'application inverse Π_P^{-1} est appelée la *factorisation* par rapport à P. Un anneau est dit *factoriel* s'il admet une structure factorielle.

Un anneau factoriel et forcément intègre. En général il peut être difficile à déterminer si un anneau intègre donné est factoriel ou non. Pour les anneaux euclidiens ou principaux, par contre, la question devient facile. Si vous l'avez déjà vu dans votre cours d'algèbre, essayez de redémontrer le théorème suivant :

Théorème 4.2. *Tout anneau euclidien est principal. Tout anneau principal est factoriel.*

Exercice 4.3. En déduire en particulier que l'anneau $\mathbb{Z}$ est factoriel, comme énoncé au début de ce chapitre. Pour la structure factorielle on choisit typiquement l'ensemble des nombres premiers *positifs*. (Vérifier que l'on pourrait aussi choisir des signes différents.) *Attention.* — On pourrait être tenté de prendre la factorialité de $\mathbb{Z}$ comme une évidence. Ce n'est pas du tout le cas. On explicitera un anneau non factoriel plus bas.

Exercice 4.4. Soit A un anneau avec une structure factorielle P. Vérifier que $\Pi_P\colon A^\times \times \mathbb{N}^{(P)} \to A^*$ est un isomorphisme de monoïdes. (Rappeler d'abord les lois sur $A^\times \times \mathbb{N}^{(P)}$ et sur A^*.) Montrer qu'une structure factorielle $P \subset A$ consiste d'éléments irréductibles. Chaque élément irréductible de A est associé à exactement un élément de P. Ainsi P est un *système de représentants* des éléments irréductibles de A.

Exercice 4.5. Vérifier que pour toute application $\varepsilon\colon P \to A^\times$ l'ensemble $\varepsilon P = \{\varepsilon(p)\cdot p \mid p \in P\}$ donne également une structure factorielle. Réciproquement, si P et P' sont deux structures factorielles sur A, alors il existe $\varepsilon\colon P \to A^\times$ de sorte que $P' = \varepsilon P$. Conclusion : s'il existe une structure factorielle sur A elle est essentiellement unique (à multiplication par des inversibles près).

Exercice 4.6. Dans beaucoup d'anneaux qui apparaissent dans la nature c'est la *non-unicité* de la factorisation qui empêche la factorialité, c'est-à-dire que Π_P est surjectif mais non injectif. Vous rencontrerez de tels anneaux dans votre cours d'algèbre. En voici un exemple simple : les polynômes $p \in \mathbb{R}[X]$ vérifiant $p'(0) = 0$ forment un sous-anneau $A \subset \mathbb{R}[X]$. Les polynômes X^2 et X^3 sont irréductibles dans A. (Pourquoi ?) Par conséquent X^6 admet *deux factorisations distinctes* en facteurs irréductibles dans A, à savoir $X^6 = X^2X^2X^2$ et $X^6 = X^3X^3$.

Exercice 4.7. Montrer le lemme d'Euclide dans un anneau factoriel : si $\operatorname{pgcd}(a,b) = 1$ et $b \mid ac$, alors $b \mid c$. En déduire tout élément irréductible est premier. Sans factorialité, il n'en est rien : dans l'anneau A de l'exemple précédent, X^2 est irréductible mais non premier : on a $X^2 | X^3X^3$ sans que $X^2 | X^3$. De même $X^3 | X^2X^4$ sans que $X^3 | X^2$ ou $X^3 | X^4$.

Exemple 4.8. Remarquons finalement que $\mathbb{Z}[\sqrt{-5}]$ est intègre mais non factoriel : on peut vérifier que 3 et $2\pm\sqrt{-5}$ sont irréductibles, et que $9 = 3\cdot 3 = (2+\sqrt{-5})\cdot(2-\sqrt{-5})$ sont deux décompositions distinctes. On voit dans cet exemple que les éléments irréductibles 3 et $2\pm\sqrt{-5}$ ne sont pas premiers (le détailler).

4.2. Aspects algorithmiques. Supposons que A admet une structure factorielle P. Il est en général facile d'évaluer l'application $\Pi_P\colon A^\times \times \mathbb{N}^{(P)} \to A^*$, car il ne s'agit que des multiplications. Par contre, l'application inverse $\Pi_P^{-1}\colon A^* \to A^\times \times \mathbb{N}^{(P)}$ peut être très difficile à calculer sur des exemples concrets ! On verra que c'est déjà très dur dans l'anneau $\mathbb{Z}$, problème qui nous occupera dans le chapitre XI.

Exercice 4.9. Vérifier que dans un anneau factoriel les formules données au début du chapitre,

$$\operatorname{pgcd}\bigl(u\textstyle\prod p^{\nu(p)}, u'\prod p^{\nu'(p)}\bigr) = \prod p^{\min(\nu(p),\nu'(p))} \quad \text{et}$$
$$\operatorname{ppcm}\bigl(u\textstyle\prod p^{\nu(p)}, u'\prod p^{\nu'(p)}\bigr) = \prod p^{\max(\nu(p),\nu'(p))},$$

définissent bien un pgcd et un ppcm. À noter en particulier que le choix de P spécifie un pgcd et un ppcm *préféré* et enlève ainsi l'ambiguïté notoire dans la définition d'un pgcd et d'un ppcm. Plus généralement, on peut définir $\operatorname{pref}\colon A^* \to A^*$ par $\operatorname{pref}(u\prod p^{\mu(p)}) = \prod p^{\mu(p)}$ ce qui choisit un représentant préféré dans chaque classe d'éléments associés. Cette construction a le bon goût d'être multiplicative, $\operatorname{pref}(xy) = \operatorname{pref}(x)\cdot\operatorname{pref}(y)$.

The source of all great mathematics is the special case, the concrete example.
It is frequent in mathematics that every instance of a concept of seemingly
great generality is in essence the same as a small and concrete special case.
Paul Halmos, *I Want to be a Mathematician*

PROJET IX

L'algorithme de Gauss-Bézout et les diviseurs élémentaires

Objectif. Nous souhaitons résoudre un *système d'équations linéaires* sur les entiers :

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= y_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= y_2 \\ & \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= y_m \end{cases}$$

Ici les coefficients a_{ij} et y_i sont des entiers et l'on cherche les solutions x_i également dans les entiers. En algèbre linéaire on développe la théorie de ces systèmes sur un corps $\mathbb{K}$, et on apprend certaines méthodes pour leur résolution, notamment la méthode de Gauss rappelée plus bas. Dans notre situation nous devons adapter cet algorithme pour tenir compte du fait que l'on ne puisse pas toujours diviser par un pivot a_{ij}. On verra comment l'algorithme d'Euclide-Bézout résout ce problème. Cette observation aboutit au théorème des diviseurs élémentaires et sa version effective, l'algorithme de Gauss-Bézout. Ce résultat classique est déjà très intéressant en lui-même, et il résout en particulier notre système d'équations linéaires.

Remarquons en passant que le théorème des diviseurs élémentaires sera tout aussi intéressant à plus long terme car il se généralise à tout anneau euclidien, notamment l'anneau des polynômes $\mathbb{K}[X]$ sur un corps $\mathbb{K}$, ou plus généralement à tout anneau principal. Comme application importante on en déduira la classification des groupes abéliens finis, ou plus généralement des modules finiment engendrés sur un anneau principal. Ne vous inquiétez pas si ces termes ne vous parlent pas encore pour le moment : c'est juste le vocabulaire général pour les observations que nous dégagerons ici sur l'anneau des entiers $\mathbb{Z}$.

Aperçu de l'approche. Comme vous en avez l'habitude, la matrice $A = (a_{ij})_{j=1,\dots,n}^{i=1,\dots,m}$ et les vecteurs $x = (x_j)_{j=1,\dots,n}$ et $y = (y_i)_{i=1,\dots,m}$ permettent d'écrire notre système plus succinctement comme $Ax = y$. Ayant fixé la matrice $A \in \mathbb{Z}^{m\times n}$ et le vecteur $y \in \mathbb{Z}^m$, il s'agit de trouver les solutions $x \in \mathbb{Z}^n$ vérifiant $Ax = y$. C'est bien plus qu'une notation commode : cette structuration des données est le point de départ de tous les algorithmes pour la résolution de systèmes linéaires.

Remarquons d'abord que le problème devient trivial si la matrice A est *diagonale*, c'est-à-dire $a_{ij} = 0$ pour toute paire d'indices $i \neq j$. Dans ce cas nos équations $a_{ii}x_i = y_i$ sont découplées les unes des autres, ce qui ramène le calcul à l'anneau de base $\mathbb{Z}$: l'existence d'une solution $x_i \in \mathbb{Z}$ revient à une question de divisibilité $a_{ii} \mid y_i$, et dans le cas favorable l'unique solution est $x_i = y_i/a_{ii}$.

Signalons quelques cas exceptionnels évidents. Si $a_{ii} = y_i = 0$, alors on a bien $a_{ii} \mid y_i$ et tout $x_i \in \mathbb{Z}$ est solution de l'équation $a_{ii}x_i = y_i$. De manière analogue, si $m < n$, alors les variables $x_{m+1}, \dots, x_n \in \mathbb{Z}$ peuvent être choisies arbitrairement. Dans le cas contraire $m > n$ notre système diagonal admet une solution seulement si les coefficients $y_{n+1}, \dots, y_m \in \mathbb{Z}$ s'annulent. (Le détailler.)

Dans le cas général l'idée est de se ramener à un système diagonal, en passant de la matrice donnée A à une matrice diagonale $D = SAT$ où S et T sont des matrices inversibles, dites *matrices de passage*. L'algorithme de Gauss-Bézout nous permet de calculer de telles matrices D, S et T, et le théorème des diviseurs élémentaires affirme que la matrice diagonale D est unique dans un certain sens.

Sommaire

1. L'algorithme de Gauss-Bézout

1.1. Calcul matriciel. Fixons deux nombres naturels $m,n \in \mathbb{N}$ et posons $I = \{1,\dots,m\}$ ainsi que $J = \{1,\dots,n\}$. Une *matrice* de taille $m \times n$ à coefficient dans $\mathbb{K}$ est une famille $A = (a_{ij})$ d'éléments $a_{ij} \in \mathbb{K}$ indexés par $(i,j) \in I \times J$. Ce n'est rien autre qu'une application $a\colon I \times J \to \mathbb{K}$ notée $(i,j) \mapsto a_{ij}$. L'ensemble de ces matrices sera noté $\mathbb{K}^{m\times n}$ ou bien $\mathrm{Mat}(m \times n;\mathbb{K})$.

Notation. Dans la pratique une telle matrice A s'écrit comme un schéma rectangulaire, avec i indexant les lignes et j indexant les colonnes. Dans cette écriture les matrices $m \times 1$ sont les vecteurs colonnes, alors que les matrices $1 \times n$ sont les vecteurs lignes. À chaque matrice $A = (a_{ij})_{ij}$ de taille $m \times n$ on peut associer la matrice transposée $A^t = (a_{ij})_{ji}$ de taille $n \times m$.

Jusqu'ici $\mathbb{K}$ puis $\mathbb{K}^{m\times n}$ n'est qu'un ensemble sans structure spécifique. La théorie devient intéressante quand $\mathbb{K}$ est un anneau : dans ce cas on peut définir une addition et une multiplication :

$$+\colon \mathbb{K}^{m\times n} \times \mathbb{K}^{m\times n} \to \mathbb{K}^{m\times n}, \quad (A,B) \mapsto C = A+B \quad \text{avec } c_{ij} = a_{ij} + b_{ij}, \tag{1}$$

$$*\colon \mathbb{K}^{m\times n} \times \mathbb{K}^{n\times r} \to \mathbb{K}^{m\times r}, \quad (A,B) \mapsto C = A*B \quad \text{avec } c_{ik} = \textstyle\sum_{j=1}^{n} a_{ij}b_{jk}. \tag{2}$$

En particulier on obtient une action des matrices sur les vecteurs par l'application $*\colon \mathbb{K}^{m\times n} \times \mathbb{K}^n \to \mathbb{K}^m$ avec $(A,x) \mapsto y = Ax$ défini par $y_i = \sum_{j=1}^{n} a_{ij}x_j$. En plus on a la multiplication scalaire (à gauche)

$$\cdot\colon \mathbb{K} \times \mathbb{K}^{m\times n} \to \mathbb{K}^{m\times n}, \quad (\lambda,A) \mapsto B = \lambda A \quad \text{avec } b_{ij} = \lambda a_{ij}. \tag{3}$$

Toutes ces notions apparaissent naturellement en algèbre linéaire, où les matrices sont un outil formidable pour représenter les applications linéaires. On suppose connu ce contexte, et on se servira du langage associé sans rentrer dans les détails d'une révision plus complète.

Exercice/M 1.1 (structure additive). L'ensemble $\mathbb{K}^{m\times n}$ muni de l'addition (1) forme un groupe abélien. L'élément neutre est la matrice nulle, notée $0_{m\times n}$ ou 0 simplement. La multiplication scalaire fait de $\mathbb{K}^{m\times n}$ un espace vectoriel sur $\mathbb{K}$. Cette terminologie suppose que $\mathbb{K}$ est un corps. — Si $\mathbb{K}$ est un anneau on exprime le même constat par des mots différents : on dit plus prudemment que $\mathbb{K}^{m\times n}$ est un module sur l'anneau $\mathbb{K}$.

Exercice/M 1.2 (structure multiplicative). La multiplication (2) est associative et admet pour élément neutre à gauche la matrice identité $1_{m\times m}$, ainsi que pour élément neutre à droite la matrice identité $1_{n\times n}$. La multiplication est distributive sur l'addition. (La matrice identité $1_{n\times n}$ est aussi notée 1_n ou simplement 1 si la dimension n est claire par le contexte.)

Exercice/M 1.3 (structure d'anneau). L'ensemble $\mathbb{K}^{n\times n}$ des matrices carrées de taille $n \times n$ sur $\mathbb{K}$ muni de l'addition et de la multiplication définies ci-dessus forme un anneau. L'application $\mathbb{K} \to \mathbb{K}^{n\times n}$, $\lambda \mapsto \lambda 1_{n\times n}$ est un isomorphisme entre notre anneau de base $\mathbb{K}$ et le sous-anneau $\mathbb{K}1_{n\times n} = \{\lambda 1_{n\times n} \mid \lambda \in \mathbb{K}\}$. Dans le cas particulier $n = 1$ on retrouve l'isomorphisme évident $\mathbb{K} \cong \mathbb{K}^{1\times 1}$. Pour $n \geq 2$ l'anneau $\mathbb{K}^{n\times n}$ est non commutatif, même si l'anneau de base $\mathbb{K}$ l'est.

Puisque $\mathbb{K}^{n\times n}$ est un anneau (non commutatif), on peut appliquer le vocabulaire usuel. Rappelons en particulier la notion d'élément inversible, qui joue toujours un rôle très important :

Définition 1.4. On dit qu'une matrice $A \in \mathbb{K}^{n\times n}$ est *inversible* dans $\mathbb{K}^{n\times n}$ s'il existe une matrice $B \in \mathbb{K}^{n\times n}$ telle que $AB = BA = 1$. Dans ce cas l'élément B est unique, on l'appelle *l'inverse* de A, et on le note A^{-1}. Les éléments inversibles de $\mathbb{K}^{n\times n}$ forment un groupe, appelé *groupe linéaire* et noté $\mathrm{GL}(n;\mathbb{K})$ ou $\mathrm{GL}_n(\mathbb{K})$.

Tout ce que l'on vient de dire est vrai pour tout anneau $\mathbb{K}$, supposé associatif et unitaire, non forcément commutatif. Dans votre cours d'algèbre linéaire vous trouvez un développement beaucoup plus complet sous l'hypothèse que $\mathbb{K}$ est un corps, c'est-à-dire un anneau unitaire commutatif dans lequel tout élément non nul est inversible. Certains résultats s'étendent encore aux anneaux commutatifs :

Théorème 1.5 (existence et unicité du déterminant)**.** *Soit $\mathbb{K}$ un anneau commutatif unitaire. Pour tout $n \in \mathbb{N}$ il existe une et une seule application* det$\colon \mathbb{K}^{n\times n} \to \mathbb{K}$, *appelée* déterminant, *qui soit alternée et multilinéaire par rapport aux colonnes et normée dans le sens que* $\det(1_{n\times n}) = 1_{\mathbb{K}}$. *Elle jouit des propriétés suivantes :*

(1) *Le déterminant se développe en la formule polynomiale* $\det A = \sum_{\sigma\in S_n} \mathrm{sign}(\sigma)\cdot a_{1,\sigma(1)}\cdot a_{2,\sigma(2)}\cdots a_{n,\sigma(n)}$ *où σ parcourt toutes les permutations dans le groupe symétrique S_n.*

(2) *Le déterminant est invariant par transposition, c'est-à-dire il satisfait* $\det(A^t) = \det(A)$. *Par conséquent il est également alterné et multilinéaire par rapport aux lignes.*

(3) *Le déterminant est multiplicatif dans le sens que* $\det(AB) = \det(A)\det(B)$. *Par restriction on obtient donc un homomorphisme de groupes* $\det\colon \mathrm{GL}_n(\mathbb{K}) \to \mathbb{K}^\times$, *manifestement surjectif.*

(4) *Une matrice A est inversible dans* $\mathbb{K}^{n\times n}$ *si et seulement si* $\det(A)$ *est inversible dans* $\mathbb{K}$. *(Ici « ⇒ » est claire ; pour « ⇐ » il existe une formule polynomiale qui exprime* A^{-1} *en fonction de A.)*

Si vous connaissez ce résultat pour les corps, vous êtes vivement invités à le redémontrer dans le cadre général des anneaux commutatifs. À noter que ce théorème n'est plus valable pour un anneau $\mathbb{K}$ non commutatif ; dégager donc bien les arguments de la preuve qui se servent de la commutativité.

Corollaire 1.6. *L'ensemble* $\mathrm{SL}_n(\mathbb{K}) = \{A \in \mathbb{K}^{n\times n} \mid \det(A) = 1\}$ *est un sous-groupe de* $\mathrm{GL}_n(K)$. □

Remarque 1.7. L'application $\det\colon \mathbb{K}^{n\times n} \to \mathbb{K}$ est multiplicative, mais pour $n \geq 2$ elle n'est pas additive : il ne s'agit pas d'un homomorphisme d'anneaux ! (Donner un contre-exemple de matrices 2×2.)

1.2. L'algorithme de Gauss-Bézout. Ce paragraphe présente l'algorithme de Gauss-Bézout pour transformer une matrice A en une matrice diagonale $D = SAT$. L'algorithme comme nous le décrivons est suffisamment efficace pour être intéressant dans la pratique ; on discutera l'implémentation plus bas.

Nous allons d'abord expliciter un sous-algorithme qui permet d'éliminer la première colonne de notre matrice A. Considérons la première ligne a_1 et la $i$ème ligne a_i : les éléments en tête sont $x = a_{11}$ et $y = a_{i1}$, respectivement. On calcule leur pgcd d avec des coefficients de Bézout $u, v \in \mathbb{Z}$ de sorte que

$$d = \mathrm{pgcd}(x,y) = ux + vy.$$

Ces données nous permettent de définir la matrice

$$M := \begin{pmatrix} u & v \\ -y/d & x/d \end{pmatrix}.$$

Elle est à coefficients entiers puisque d est un diviseur commun de x et y. Par sa construction elle vérifie $M\binom{x}{y} = \binom{d}{0}$ ainsi que $\det(M) = 1$. (Le vérifier.) Son inverse est d'ailleurs facile à expliciter :

$$M^{-1} = \begin{pmatrix} x/d & -v \\ y/d & u \end{pmatrix}.$$

On peut maintenant appliquer la matrice M aux lignes a_1 et a_i, ce qui revient à calculer $a'_1 \leftarrow ua_1 + va_i$ puis $a'_i \leftarrow -\frac{y}{d}a_1 + \frac{x}{d}a_i$. Dans la nouvelle matrice A' le coefficient a'_{i1} s'annule comme souhaité. En parcourant $i = 2, \ldots, m$ on peut ainsi éliminer la première colonne. Les mêmes arguments se transposent aux opérations sur les colonnes, ce qui permet d'éliminer la première ligne. En voici un exemple détaillé :

Exemple 1.8. Essayons de mettre sous forme diagonale la matrice

$$A_0 = \begin{pmatrix} 48 & 12 & 18 \\ 36 & 21 & 9 \end{pmatrix}.$$

Pour les coefficients $x = 48$ et $y = 36$ dans la première colonne on trouve $d = \mathrm{pgcd}(x,y) = 12$ avec des coefficients de Bézout $u = 1$ et $v = -1$ vérifiant $d = ux + vy$. Ceci nous mène à

$$M_0 := \begin{pmatrix} 1 & -1 \\ -3 & 4 \end{pmatrix} \quad \text{puis} \quad A_1 := M_0 A_0 = \begin{pmatrix} 12 & -9 & 9 \\ 0 & 48 & -18 \end{pmatrix}.$$

Nous éliminons ensuite la première ligne de la même façon. Pour les coefficients $x = 12$ et $y = -9$ dans la première ligne nous trouvons $d = 3$ ainsi que $u = 1$ et $v = 1$. Puisque nous effectuons maintenant les transformations sur les colonnes, ceci se traduit par multiplier A à droite :

$$M_1 := \begin{pmatrix} 1 & 3 & 0 \\ 1 & 4 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{donne} \quad A_2 := A_1 M_1 = \begin{pmatrix} 3 & 0 & 9 \\ 48 & 192 & -18 \end{pmatrix}.$$

Pour $x = 3$ et $y = 9$ on trouve $d = 3$ ainsi que $u = 1$ et $v = 0$, donc la transformation par

$$M_2 := \begin{pmatrix} 1 & 0 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{donne} \quad A_3 := A_2 M_2 = \begin{pmatrix} 3 & 0 & 0 \\ 48 & 192 & -162 \end{pmatrix}.$$

On vient d'éliminer la première ligne, mais en contrepartie on a gâché un peu la première colonne. Restons optimiste et recommençons : pour $x = 3$ et $y = 48$ on trouve $d = 3$ ainsi que $u = 1$ et $v = 0$, donc

$$M_3 := \begin{pmatrix} 1 & 0 \\ -16 & 1 \end{pmatrix} \quad \text{donne} \quad A_4 := M_3 A_3 = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 192 & -162 \end{pmatrix}.$$

Nous avons finalement éliminé à la fois la première colonne *et* la première ligne. Nous pouvons passer à la sous-matrice qui reste : pour $x = 192$ et $y = -162$ nous trouvons $d = 6$ ainsi que $u = 11$ et $v = 13$:

$$M_4 := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 11 & 27 \\ 0 & 13 & 32 \end{pmatrix} \quad \text{donne} \quad A_5 := A_4 M_4 = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 6 & 0 \end{pmatrix}.$$

Ceci termine l'algorithme. Mettant tout ensemble, on obtient ainsi les matrices de passage

$$S := M_3 M_0 = \begin{pmatrix} 1 & -1 \\ -19 & 20 \end{pmatrix} \quad \text{et} \quad T := M_1 M_2 M_4 = \begin{pmatrix} 1 & -6 & -15 \\ 1 & 5 & 12 \\ 0 & 13 & 32 \end{pmatrix} \quad \text{vérifiant} \quad SAT = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 6 & 0 \end{pmatrix}.$$

Remarque 1.9 (matrices de passage)**.** Afin de construire les matrices de passage S et T lors du calcul, on commence par les matrices $S_0 = 1_{m\times m}$ et $T_0 = 1_{n\times n}$ vérifiant $A_0 = S_0 A T_0$.

- Une opération sur les lignes correspond à une multiplication à gauche : $A_{k+1} := M_k A_k$ avec une matrice inversible M_k comme ci-dessus. On pose $S_{k+1} := M_k S_k$ et $T_{k+1} := T_k$.
- Une opération sur les colonnes correspond à une multiplication à droite : $A_{k+1} := A_k M_k$avec une matrice inversible M_k comme ci-dessus. On pose $S_{k+1} := S_k$ et $T_{k+1} := T_k M_k$.

Dans les deux cas on part de $A_k = S_k A T_k$ et on assure que $A_{k+1} = S_{k+1} A T_{k+1}$. Chaque transformation correspond à une matrice M_k de déterminant $+1$. Ceci assure que les matrices de passages S_k et T_k sont également de déterminant $+1$. L'algorithme se termine avec une matrice diagonale $D = A_k$ pour un certain k. Avec $S = S_k$ et $T = T_K$ on obtient $D = SAT$ comme souhaité.

En guise de résumé, voici la version concise de l'algorithme de Gauss-Bézout. Pour le moment nous entendons par *forme normale* une forme diagonale quelconque. Ceci sera précisé plus loin par une condition supplémentaire.

Algorithme IX.4 Algorithme de Gauss-Bézout

Entrée: une matrice $A \in \mathbb{Z}^{m\times n}$

Sortie: trois matrices $D \in \mathbb{Z}^{m\times n}$, $S \in \mathbb{Z}^{m\times m}$, $T \in \mathbb{Z}^{n\times n}$ telles que $D = SAT$

Garanties: D est sous forme normale et S et T sont inversibles de déterminant 1.

Initialiser $D \leftarrow A$ et $S \leftarrow 1_{m\times m}$ et $T \leftarrow 1_{n\times n}$	// On assure $D_0 = S_0 A T_0$.
tant que D n'est pas encore sous forme normale **faire**	
Effectuer une transformation sur deux lignes ou deux colonnes	// On s'approche du résultat souhaité.
Mettre à jour les matrices de passages S et T	// $D_k = S_k A T_k \Rightarrow D_{k+1} = S_{k+1} A T_{k+1}$.
fin tant que	
retourner (D, S, T)	// $D_k = S_k A T_k$ est sous forme normale.

1.3. Preuve de correction. L'algorithme de Gauss-Bézout a bien marché sur l'exemple précédent. Montrons que l'approche réussit toujours :

Proposition 1.10. *Les opérations élémentaires sur les lignes et les colonnes permettent de transformer toute matrice $A \in \mathbb{K}^{m\times n}$ en une matrice A' telle que $a'_{i1} = a'_{1j} = 0$ pour tout $i, j \geq 2$.*

DÉMONSTRATION. On descend d'abord la première colonne ; les opérations sur les lignes décrites ci-dessus permettent d'obtenir $a_{i1} = 0$. Ensuite on traverse la première ligne pour obtenir $a_{1j} = 0$. Or, ces dernières opérations ajoutent des multiples des colonnes $j \geq 2$ à la première colonne. Par conséquent on ne préserve en général pas la condition $a_{i1} = 0$ et on est obligé de repasser la première colonne, puis la première ligne, etc.

Heureusement ce processus se termine après un nombre fini d'itérations : dans chaque opération le coefficient a_{11} est remplacé par un de ses diviseurs, a savoir $\operatorname{pgcd}(a_{11}, a_{ij})$ où a_{ij} est le coefficient que l'on

cherche à annuler. Ceci ne peut modifier la valeur de a_{11} qu'un nombre fini de fois. S'il ne change plus, ceci veut dire que a_{11} divise tous les coefficients a_{i1} de la première colonne ainsi que tous les coefficients a_{1j} de la première ligne. On arrive ainsi au cas simple de l'algorithme usuel sur un corps : avec $d = a_{11}$, $u = 1$, $v = 0$ la transformation revient à calculer $A'_i \leftarrow A_i - \frac{a_{i1}}{a_{11}} A_1$ sans changer la ligne A_1, et il en est de même pour les opérations sur les colonnes. Après ce dernier passage on obtient l'annulation souhaitée. □

Proposition 1.11. *Les opérations élémentaires sur les lignes et les colonnes permettent de transformer toute matrice $A \in \mathbb{K}^{m\times n}$ en une matrice diagonale D, c'est-à-dire $d_{ij} = 0$ pour toute paire d'indices $i \neq j$. En plus on peut assurer la divisibilité successive $d_{11} \mid d_{22} \mid d_{33} \mid \dots$ des termes diagonaux.*

DÉMONSTRATION. Supposons que $m \leq n$. Pour $k = 1, \dots, m$ on applique la proposition précédente à la sous-matrice indexée par des paires (i, j) avec $i, j \geq k$. Pour $k = 1$ on élimine ainsi la première ligne et la première colonne. Pour $k = 2$ on élimine la seconde ligne et la seconde colonne de la sous-matrice, et ainsi de suite. Le résultat final est une matrice D dont tous les coefficients hors de la diagonale s'annulent.

Étant donné deux termes diagonaux $x, y \in \mathbb{Z}$ on calcule à nouveau $d := \text{pgcd}(x, y) = ux + vy$ avec des coefficients de Bézout $u, v \in \mathbb{Z}$. On a $e := \text{ppcm}(x, y) = xy/d$, et on vérifie aisément que

$$\begin{pmatrix} u & v \\ -y/d & x/d \end{pmatrix} \cdot \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \cdot \begin{pmatrix} 1 & -vy/d \\ 1 & ux/d \end{pmatrix} = \begin{pmatrix} d & 0 \\ 0 & e \end{pmatrix}.$$

Les deux matrices de passage sont inversibles car de déterminant 1. En traversant ainsi toute la diagonale on peut assurer que d_{11} soit le pgcd de tous les termes diagonaux. Ensuite on réitère pour assurer que d_{22} soit le pgcd de tous les termes diagonaux suivants, et ainsi de suite. □

1.4. Implémentation. Dans le développement mathématique nous avons utilisé certaines matrices M qui représentent des opérations sur les lignes ($A' \leftarrow MA$) ou les colonnes ($A' \leftarrow AM$). On pourrait l'implémenter littéralement, c'est-à-dire, construire la matrice M puis faire appel à la multiplication des matrices. Or, la matrice M est très creuse : c'est presque la matrice identité, avec seulement quatre coefficients potentiellement non triviaux. Nous allons donc implémenter les transformations élémentaires par deux fonctions spécialisées comme suit :

```
void gauss_gauche( const Integer& a, const Integer& b,
                   const Integer& c, const Integer& d,
                   Matrix<Integer>& mat, int i, int j, int k=1 );

void gauss_droite( const Integer& a, const Integer& b,
                   const Integer& c, const Integer& d,
                   Matrix<Integer>& mat, int i, int j, int k=1 );
```

Ici la matrice $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ opère sur les lignes/colonnes i et j de la matrice A. Par souci d'efficacité on songe déjà au cas d'une réduction plus évoluée, où les $k-1$ premières lignes et colonnes sont déjà diagonalisées et ne jouent plus de rôle. Puisqu'il ne sert à rien de manipuler des zéros, les opérations ci- dessus ne s'appliquent qu'à la sous-matrice $i, j \geq k$. Ainsi les fonctions suivantes annulent la ligne ou colonne k :

```
bool gauss_colonne( Matrix<K>& mat, Matrix<K>& s, Dim k );
bool gauss_ligne( Matrix<K>& mat, Matrix<K>& t, Dim k );
```

Exercice/P 1.12. En suivant le modèle `gauss-bezout.cc`, implémenter efficacement l'algorithme de Gauss-Bézout en une fonction

```
void gauss_bezout( Matrix<K>& mat, Matrix<K>& s, Matrix<K>& t );
```

Ici `mat` contient la matrice initiale qui sera transformée à fur et à mesure en une matrice diagonale, en modifiant directement la matrice `mat`. Les matrices `s` et `t` sont initialisées par les matrices identités convenables. On fait agir les opérations à gauche sur `s` et les opérations à droite sur `t` comme ci-dessus.

Exercice/P 1.13. Testez votre implémentation sur des matrices variées. Comment peut-on vérifier efficacement les résultats ? Est-ce que votre implémentation est suffisamment efficace pour des matrices denses aléatoires de taille 10×10 ? 20×20 ? 50×50 ? 100×100 ? Quels phénomènes observez-vous ?

Remarque 1.14 (résolution d'un système linéaire)**.** L'algorithme de Gauss-Bézout résout notre problème initial d'un système $Ax = y$. On passe à la matrice diagonale $D = SAT$, puis le système diagonal $D\hat{x} = \hat{y}$ se résout aisément. Ici on pose $\hat{y} = Sy$, et la solution x s'obtient ensuite par $x = T\hat{x}$.

1.5. Calcul efficace du déterminant. Rappelons que dans le théorème du déterminant énoncé ci-dessus, l'unicité et l'existence du déterminant sont établies par la formule explicite

$$\det A = \sum_{\sigma\in S_n} \operatorname{sign}(\sigma)\cdot a_{1,\sigma(1)}\cdot a_{2,\sigma(2)}\cdots a_{n,\sigma(n)}.$$

Traduite littéralement, cette formule donne un algorithme de complexité $n!$ ce qui n'est pas du tout efficace pour n grand. (Calculer 10! ou 20! voire 50! pour vous en convaincre.) Le développement récursif par rapport à une ligne ou une colonne n'est qu'une reformulation de cette approche, et donc aussi inefficace. Le seul cas lucratif est le développement par rapport à une ligne ou une colonne *creuse*, c'est-à-dire contenant peu de coefficients non nuls.

Dans le cas général d'une grande matrice dense, l'algorithme de Gauss-Bézout se révèle plus avantageux, à savoir de complexité d'environ n^3 opérations dans $\mathbb{K}$. Un problème notoire est « l'explosion des coefficients » lors des calculs intermédiaires. Soulignons que le nombre d'opérations dans $\mathbb{K}$ n'est qu'une indication grossière : les opérations dans $\mathbb{Z}$ deviennent plus coûteuses en temps et en mémoire quand les coefficients grandissent. Quelques exemples sur des matrices aléatoires vous convaincront que ce phénomène est bien réel, même si la matrice initiale n'a que des coefficients de petite taille.

Bien sûr, une explosion des coefficients ne peut se produire que dans un anneau infini. Une astuce éprouvée est donc de réduire modulo un nombre premier p afin d'effectuer le calcul dans le corps fini $\mathbb{Z}_p$. Pour reconstituer le résultat dans $\mathbb{Z}$ on rassemble l'information modulo plusieurs nombres premiers $p_1, p_2, \ldots$. Pour un développement de cette idée voir Gathen-Gerhard [**11**], §5.5.

1.6. Le théorème des diviseurs élémentaires. D'après ce qui précède on sait maintenant transformer une matrice donnée A en une matrice diagonale D : l'algorithme de Gauss-Bézout ci-dessus en explicite une démarche. Il y a pourtant de nombreux choix : d'autres manières de procéder sont imaginables et leurs matrices de passages seront très différentes. Le résultat suivant est donc tout à fait remarquable : il dit que la matrice diagonale qui en résulte est toujours la même :

Théorème 1.15 (le théorème des diviseurs élémentaires)**.** *Pour toute matrice $A \in \mathrm{Mat}(m\times n;\mathbb{Z})$ il existe des matrices inversibles $S \in \mathrm{SL}_m(\mathbb{Z})$ et $T \in \mathrm{SL}_n(\mathbb{Z})$ telles que la matrice produit $D = SAT$ soit diagonale et vérifie la divisibilité successive $d_{11} \mid d_{22} \mid d_{33} \mid \ldots$ des termes diagonaux. Dans ce cas ces termes sont uniques aux signes près : pour toute autre diagonalisation $D' = S'AT'$ avec $S' \in \mathrm{SL}_m(\mathbb{Z})$ et $T' \in \mathrm{SL}_n(\mathbb{Z})$ satisfaisant la condition $d'_{11} \mid d'_{22} \mid d'_{33} \mid \ldots$ on a $d'_{ii} = \pm d_{ii}$ pour tout i.*

Définition 1.16. Une matrice $D \in \mathbb{Z}^{m\times n}$ est sous *forme normale* si elle est diagonale et ses termes diagonaux vérifient $d_{11} \mid d_{22} \mid d_{33} \mid \ldots$. Le théorème des diviseurs élémentaires dit que toute matrice $A \in \mathbb{Z}^{m\times n}$ peut être mise sous forme normale. On appelle *diviseurs élémentaires* de A la suite $d_{11} \mid d_{22} \mid d_{33} \mid \ldots$ dont l'existence et l'unicité (aux signes près) sont assurées par le théorème précédent.

Remarque 1.17. Pour la fonction `pgcd` nous avons tacitement fait usage de notre convention : *le* pgcd de deux entiers est entendu comme le pgcd *positif*. Ainsi la matrice D retournée par notre algorithme satisfait à la condition $d_{11} \mid d_{22} \mid d_{33} \mid \ldots$ avec des termes diagonaux *positifs*, à l'exception éventuelle du dernier. Ainsi le signe du déterminant est retenu dans le tout dernier terme diagonal.

1.7. Unicité du résultat. Dans l'algorithme de Gauss-Bézout on a plusieurs choix : déjà les coefficients de Bézout utilisés à chaque étape ne sont pas uniques, puis l'ordre par lequel on effectue les opérations n'est pas canonique. Les matrices de passages S et T obtenues à la fin dépendent de ces choix et ne sont pas du tout uniques. On pourrait même imaginer des approches totalement différentes pour mettre une matrice A sous une forme diagonale. Il n'y a donc a priori aucune raison de croire que le résultat soit canonique. Des exemples simples, comme le suivant, montrent que les termes diagonaux peuvent changer :

$$A = \begin{pmatrix} 4 & 0 \\ 0 & 6 \end{pmatrix} \quad \text{se transforme en} \quad SAT = \begin{pmatrix} 2 & 0 \\ 0 & 12 \end{pmatrix} \quad \text{avec} \quad S = \begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix} \quad \text{et} \quad T = \begin{pmatrix} 1 & 3 \\ 1 & 4 \end{pmatrix}.$$

Il est donc tout à fait remarquable que les diviseurs élémentaires soient essentiellement uniques ! Pour la preuve nous allons employer ce merveilleux outil qu'est le déterminant. Supposons que A est une matrice de taille $m\times n$. Pour $I' \subset I$ et $J' \subset J$ de cardinal $|I| = |J| = k$ nous définissons la sous-matrice $A|_{I'\times J'} = (a_{ij})_{i\in I', j\in J'}$ par restriction des indices.

Définition 1.18. On note $\Delta_k(A)$ le pgcd des déterminants de toutes les sous-matrices de taille $k \times k$ de A.

Lemme 1.19. *$\Delta_k(A)$ ne change pas lors d'une transformation élémentaire sur les lignes ou les colonnes.*

DÉMONSTRATION. Il suffit de le prouver pour une transformation sur les lignes. Regardons une matrice $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ agissant sur les lignes i et j. Si une sous-matrice B ne contient ni la ligne i ni la ligne j, alors la sous-matrice B et son déterminant $\det(B)$ ne changent pas. Si une sous-matrice B contient les deux lignes, alors la matrice B change mais non son déterminant.

Le cas intéressant est celui où une sous-matrice B contient la ligne i mais non la ligne j. Soit C la sous-matrice correspondante où l'on remplace la ligne i par la ligne j. Notons $x = \det(B)$ et $y = \det(C)$ leurs déterminants. Après transformation nous obtenons deux sous-matrices modifiées B' et C' avec déterminants $x' = \det(B')$ et $y' = \det(C')$. Par multilinéarité du déterminant on trouve $x' = ax + by$ et $y' = cx + dy$, donc les diviseurs communs de x et y sont aussi des diviseurs communs de x' et y'. La réciproque est également vraie puisque M est inversible sur $\mathbb{Z}$. Ceci veut dire que $\mathrm{pgcd}(x,y) = \mathrm{pgcd}(x',y')$. On conclut que $\Delta_k(A)$ ne change pas lors d'une transformation élémentaire, comme énoncé. □

Lemme 1.20. *Le groupe $\mathrm{SL}_n(\mathbb{Z})$ est engendré par les sous-groupes $\mathrm{SL}_2^{ij}(\mathbb{Z})$ avec $1 \leq i < j \leq n$.*

DÉMONSTRATION. Précisons d'abord la notation : une matrice $A \in \mathbb{Z}^{n\times n}$ appartient à $\mathrm{SL}_2^{ij}(\mathbb{Z})$ si la sous-matrice $\left(\begin{smallmatrix} a_{ii} & a_{ij} \\ a_{ji} & a_{jj} \end{smallmatrix}\right)$ appartient à $\mathrm{SL}_2(\mathbb{Z})$ alors que tous les autres coefficients sont ceux de la matrice identité $1_{n\times n}$. Ce sont précisément les matrices qui apparaissent dans l'algorithme de Gauss-Bézout lors des transformations élémentaires. L'énoncé découle de l'application de cet algorithme à une matrice $A \in \mathrm{SL}_n(\mathbb{Z})$ pour la transformer en une matrice diagonale $D = SAT$. Par construction les matrices S et T sont produits de matrices dans $\mathrm{SL}_2^{ij}(\mathbb{Z})$ avec $1 \leq i < j \leq n$. Puisque $D \in \mathrm{SL}_n(\mathbb{Z})$ on a $d_{ii} = \pm 1$, et avec notre convention de signes on a même $D = 1_{n\times n}$. □

PREUVE DU THÉORÈME. Supposons que A est une matrice diagonale de taille $m \times n$, disons avec $m \leq n$, vérifiant $a_{11} \mid a_{22} \mid \cdots \mid a_{mm}$. Cette propriété entraîne que $\Delta_1(A) = \pm a_{11}$, puis $\Delta_2(A) = \pm a_{11}a_{22}$, … jusqu'à $\Delta_m(A) = \pm a_{11}a_{22}\cdots a_{mm}$. Supposons que l'on transforme A en une matrice diagonale $A' = SAT$ avec $S \in \mathrm{SL}_m(\mathbb{Z})$ et $T \in \mathrm{SL}_n(\mathbb{Z})$. D'après le lemme 1.20 ceci revient à effectuer des transformations élémentaires sur les lignes et les colonnes. Ceci ne change pas les invariants $\Delta_1, \ldots, \Delta_m$, ce qui permet de conclure que $a_{11} = \pm a'_{11}$, puis $a_{22} = \pm a'_{22}$, … jusqu'à $a_{mm} = \pm a'_{mm}$, comme souhaité. □

2. Applications aux groupes abéliens

2.1. Groupes abéliens libres. Pour tout groupe $(G,+)$ on a une unique application $\sigma\colon \mathbb{Z} \times G \to G$, notée $(\lambda, a) \mapsto \lambda a$, vérifiant $0a = 0$ puis $(\lambda+1)a = \lambda a + a$ pour tout $\lambda \in \mathbb{Z}$. On en déduit que $1a = a$ ainsi que $(\lambda + \lambda')a = \lambda a + \lambda' a$ et $(\lambda\lambda')a = \lambda(\lambda' a)$. Par contre, l'application σ vérifie $\lambda(a+b) = \lambda a + \lambda b$ pour tout $\lambda \in \mathbb{Z}$ et $a, b \in G$ si et seulement si G est abélien. (Exercice.) En termes savants on dit qu'un groupe abélien est un *module* sur l'anneau $\mathbb{Z}$.

Définition 2.1. Soit $(G,+)$ un groupe abélien et soit $(g_i)_{i\in I}$ une famille d'éléments $g_i \in G$ indexés par $i \in I$. Une *combinaison linéaire* (sur $\mathbb{Z}$) est une somme $\sum_{i\in I} \lambda_i g_i$ avec des coefficients entiers $\lambda_i \in \mathbb{Z}$. Si l'ensemble I est infini nous ajoutons toujours la condition que seul un nombre fini de coefficients λ_i soient non nuls. (La sommation sur une infinité de termes non nuls n'a pas de sens.)

Définition 2.2. La famille $(g_i)_{i\in I}$ est *génératrice* pour le groupe G si tout élément $g \in G$ s'écrit comme une combinaison linéaire $g = \sum_{i\in I} \lambda_i g_i$ avec $\lambda_i \in \mathbb{Z}$. On dit que G est *finiment engendré* s'il admet une famille génératrice finie $(g_1, \ldots, g_n)$.

Définition 2.3. La famille $(g_i)_{i\in I}$ dans un groupe abélien G est *libre* si la seule combinaison linéaire nulle $\sum_{i\in I} \lambda_i g_i = 0$ est la somme triviale avec $\lambda_i = 0$ pour tout $i \in I$. La famille $(g_i)_{i\in I}$ est une *base* de G si elle est génératrice et libre. Ceci équivaut à dire que tout élément $g \in G$ s'écrit de manière unique comme $g = \sum_{i\in I} \lambda_i g_i$ avec $\lambda_i \in \mathbb{Z}$. Le groupe G est *libre* s'il admet une base.

Exemple 2.4. Le groupe $\mathbb{Z}$ est libre à base 1 (ou -1). Pour tout $m \in \mathbb{N}$ le groupe $\mathbb{Z}^m$ est libre : les éléments $e_i \in \mathbb{Z}^m$ avec $e_{ij} = 0$ pour $j \neq i$ et $e_{ii} = 1$ forment une base, dite *base canonique*.

Exemple 2.5. Pour $n \geq 2$ le groupe quotient $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ n'est pas libre. Un élément $\bar{a} \in \mathbb{Z}_n$ est générateur si et seulement si $\text{pgcd}(a,n) = 1$. Il n'est pas libre car $n\bar{a} = 0\bar{a} = 0$. (Que dire des cas $n = 1$ et $n = 0$?)

Exemple 2.6. Soit I un ensemble et soit $\mathbb{Z}^{(I)}$ l'ensemble des applications $I \to \mathbb{Z}$ a support fini. C'est un groupe libre : comme base on prendra les applications $e_i \colon I \to \mathbb{Z}$ avec $e_i(j) = 0$ pour $j \neq i$ et $e_i(i) = 1$.

Proposition 2.7. *Un groupe abélien G est libre si et seulement s'il est isomorphe à un groupe $\mathbb{Z}^{(I)}$.*

DÉMONSTRATION. Si G est libre, alors il existe une base $(g_i)_{i\in I}$ et l'application $f \colon \mathbb{Z}^{(I)} \to G$ définie par $(\lambda_i)_{i\in I} \to \sum_{i\in I} \lambda_i g_i$ est un isomorphisme de groupes avec $e_i \mapsto g_i$. Réciproquement, s'il existe un isomorphisme de groupes $f \colon \mathbb{Z}^{(I)} \to G$, alors la famille $(g_i)_{i\in I}$ avec $g_i = f(e_i)$ est une base de G. □

2.2. Applications linéaires. Un homomorphisme $f \colon G \to H$ entre deux groupes abéliens est une application vérifiant $f(a+b) = f(a) + f(b)$ pour tout $a, b \in G$. Dans ce cas elle vérifie automatiquement $f(\lambda a) = \lambda f(a)$ pour tout $\lambda \in \mathbb{Z}$ et $a \in G$, et plus généralement $f(\sum_i \lambda_i a_i) = \sum_i \lambda_i f(a_i)$ pour $\lambda_i \in \mathbb{Z}$ et $a_i \in G$. (Exercice.) Au lieu d'homomorphismes de groupes abéliens on peut donc parler d'applications $\mathbb{Z}$-linéaires (ou encore d'homomorphismes de $\mathbb{Z}$-modules).

Proposition 2.8. *Soit G un groupe abélien libre à base $(g_i)_{i\in I}$. Étant donné un groupe abélien H est une famille $(h_i)_{i\in I}$ d'éléments $h_i \in H$, il existe un unique homomorphisme de groupes $f \colon G \to H$ vérifiant $f(g_i) = h_i$ pour tout $i \in I$.*

DÉMONSTRATION. *Unicité.* — Supposons que $f, f' \colon G \to H$ vérifient $f(g_i) = f'(g_i) = h_i$. Puisque $(g_i)_{i\in I}$ est une famille génératrice, tout élément $g \in G$ s'écrit comme $g = \sum_{i\in I} \lambda_i g_i$, donc $f(g) = f(\sum_i \lambda_i g_i) = \sum_i \lambda_i f(g_i) = \sum_i \lambda_i f'(g_i) = f'(\sum_i \lambda_i g_i) = f'(g)$.

Existence. — On définit $f \colon G \to H$ pour $g = \sum_{i\in I} \lambda_i g_i$ par $f(g) = \sum_{i\in I} \lambda_i h_i$. Puisque $(g_i)_{i\in I}$ est une base, tout élément $g \in G$ s'écrit ainsi de manière unique, ce qui assure que f est bien définie. L'application f est manifestement un homomorphisme de groupe qui vérifie $f(g_i) = h_i$, comme souhaité. □

Corollaire 2.9. *Soient G un groupe abélien libre à base $(g_1, \ldots, g_n)$ et H un groupe abélien libre à base $(h_1, \ldots, h_m)$. À tout homomorphisme de groupe $f \colon G \to H$ on peut associer une unique matrice $A \in \mathbb{Z}^{m\times n}$ de sorte que $f(g_j) = \sum_{i=0}^{m} a_{ij} h_i$ pour tout $j = 1, \ldots, n$. Réciproquement à toute matrice $A \in \mathbb{Z}^{m\times n}$ on peut associer un unique homomorphisme de groupe $f \colon G \to H$ vérifiant cette formule.* □

Nous regarderons dans la suite seulement des groupes abéliens finiment engendrés. C'est une restriction naturelle si l'on veut étudier des questions algorithmiques. Mais aussi mathématiquement c'est une classe beaucoup plus maniable et très importante.

Proposition 2.10. *Il existe un isomorphisme de groupes $\mathbb{Z}^n \cong \mathbb{Z}^m$ si et seulement si $n = m$.*

DÉMONSTRATION. Supposons par absurde qu'il existe un isomorphisme $f \colon \mathbb{Z}^n \xrightarrow{\sim} \mathbb{Z}^m$ pour $n > m$. Soit $A \in \mathbb{Z}^{m\times n}$ la matrice qui représente f dans les bases canoniques de $\mathbb{Z}^n$ et $\mathbb{Z}^m$. L'algorithme de Gauss-Bézout transforme A en une matrice diagonale $D = SAT$. Puisque $n > m$, la dernière colonne de D est nulle, et donc $De_n = 0$. Ainsi $A = S^{-1}DT^{-1}$ a aussi un noyau non trivial, car Te_n est envoyé sur 0. Ceci contredit l'hypothèse que f était un isomorphisme. □

Corollaire 2.11. *Si G est un groupe abélien libre avec deux bases $(g_1, \ldots, g_n)$ et $(h_1, \ldots, h_m)$ alors $n = m$. Ceci permet de définir le* rang *d'un groupe abélien libre G comme le cardinal d'une de ses bases.* □

Remarque 2.12. Vous connaissez le résultat analogue pour les espaces vectoriels sur un corps, ce qui permet de définir la *dimension*, notion puissante et omniprésente en algèbre linéaire. Pour les groupes abéliens (les modules sur $\mathbb{Z}$) il faut se restreindre aux groupes abéliens *libres* pour parler de bases. Puis la même question se pose : la notion de rang est-elle bien définie ? Nous avons choisi ici une preuve qui tire profit de l'algorithme de Gauss-Bézout.

L'énoncé se généralise à tout anneau commutatif unitaire A. Dans cette généralité la preuve ne s'applique pas telle quelle, parce que nous n'avons plus l'algorithme de Gauss-Bézout à notre disposition. Si A est intègre on peut passer à son corps des fractions. Si A n'est pas intègre on peut quotienter par un idéal maximal I : comme $F = A/I$ est un corps la preuve ci-dessus nous donne à nouveau le résultat souhaité. Si vous connaissez ces outils, vous pouvez tenter une preuve.

2.3. Sous-groupes de $\mathbb{Z}^m$. Dans ce paragraphe nous allons classifier les sous-groupes de $\mathbb{Z}^m$. Notre but sera d'abord de comprendre quels sous-groupes sont possibles, et ensuite de décrire comment ils sont plongés dans le groupe ambiant $\mathbb{Z}^m$.

Lemme 2.13. *Tout sous-groupe $H \subset \mathbb{Z}^m$ est libre et* $\operatorname{rang} H \leq m$.

DÉMONSTRATION. Nous allons établir le résultat par récurrence sur m. Pour $m = 0$ on n'a rien à montrer : le seul sous-groupe $H = \mathbb{Z}^0 = \{0\}$ est libre ayant la famille vide pour base. Si $m = 1$ nous avons un sous-groupe $H \subset \mathbb{Z}$: soit $H = \{0\}$ soit $H = \mathbb{Z}a$ pour un élément $a \in H \smallsetminus \{0\}$ de plus petite norme. (L'anneau $\mathbb{Z}$ est principal, voir la proposition 2.12.) Dans ce dernier cas la famille (a) forme une base.

Pour $m \geq 2$ soit $p\colon \mathbb{Z}^m \to \mathbb{Z}$, $(x_1, \dots, x_m) \mapsto x_m$, la projection sur la dernière coordonnée. Nous pouvons identifier $\mathbb{Z}^{m-1}$ avec le noyau $\ker(p)$ via l'application $(x_1, \dots, x_{m-1}) \mapsto (x_1, \dots, x_{m-1}, 0)$. La projection p nous permet de construire le sous-groupe $K = \ker(p|_H) = H \cap \mathbb{Z}^{m-1}$ de $\ker(p) \cong \mathbb{Z}^{m-1}$. Par hypothèse de récurrence K admet une base $v_1, \dots, v_{n-1} \in K$ de cardinal $n - 1 \leq m - 1$. L'image $p(H) \subset \mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. Si $p(H) = 0$ alors $H = K$ et il n'y a plus rien à montrer. Sinon $p(H) = \mathbb{Z}a$ pour un élément $a \in p(H) \smallsetminus \{0\}$ de plus petite norme. Soit $v_n \in H$ un élément tel que $p(v_n) = a$. Nous affirmons que $v_1, \dots, v_{n-1}, v_n$ est une base de H.

C'est une famille génératrice. — Pour tout $v \in H$ nous avons $p(v) = \lambda_n a$ avec $\lambda_n \in \mathbb{Z}$. Ainsi $v - \lambda_n v_n \in K$, et donc $v - \lambda_n v_n = \sum_{i=0}^{n-1} \lambda_i v_i$ puisque K est engendré par $v_1, \dots, v_{n-1}$ par hypothèse de récurrence.

C'est une famille libre. — Si $\sum_{i=0}^{n} \lambda_i v_i = 0$ alors $0 = p(\sum_{i=0}^{n} \lambda_i v_i) = \lambda_n a$ donc $\lambda_n = 0$. Ensuite $\sum_{i=0}^{n-1} \lambda_i v_i = 0$ entraîne $\lambda_1 = \cdots = \lambda_{n-1} = 0$ parce que la famille $v_1, \dots, v_{n-1}$ est libre par hypothèse de récurrence. □

Théorème 2.14. *Soit $H \subset \mathbb{Z}^m$ un sous-groupe. Alors il existe*

(1) *une base $b_1, \dots, b_m$ de $\mathbb{Z}^m$ et*

(2) *un entier r avec $0 \leq r \leq m$ et*

(3) *des entiers $e_1, \dots, e_r \geq 1$ vérifiant $e_1 \mid \cdots \mid e_r$*

tels que $e_1 b_1, \dots, e_r b_r$ soit une base de H. La suite des entiers $e_1, \dots, e_r$ est uniquement déterminée par H et on les appelle les diviseurs élémentaires *du sous-groupe $H \subset \mathbb{Z}^m$.*

DÉMONSTRATION. *Existence.* — Le lemme précédent nous assure l'existence d'une famille génératrice finie $v_1, \dots, v_n$. (Il n'est pas nécessaire de la supposer libre.) Ceci permet de définir une application $\mathbb{Z}$-linéaire $f\colon \mathbb{Z}^n \to \mathbb{Z}^m$ par $(\lambda_1, \dots, \lambda_n) \mapsto \lambda_1 v_1 + \cdots + \lambda_n v_n$. La matrice $A \in \mathbb{Z}^{m \times n}$ qui représente f est formée par les colonnes $v_1, \dots, v_n$. L'algorithme de Gauss-Bézout transforme A en une matrice diagonale $D = SAT$. Notons $e_1, \dots, e_r$ ses termes diagonaux non nuls et considérons $A = S^{-1} D T^{-1}$. Les colonnes $b_1, \dots, b_m$ de S^{-1} forment une base de $\mathbb{Z}^m$. Visiblement, les éléments $e_1 b_1, \dots, e_r b_r$ forment une base de l'image de A. On conclut que c'est une base de H, comme énoncé.

Unicité. — L'application $f\colon \mathbb{Z}^r \to \mathbb{Z}^m$ définie par $(\lambda_1, \dots, \lambda_r) \mapsto \lambda_1 e_1 b_1 + \cdots + \lambda_r e_r b_r$ est un isomorphisme entre $\mathbb{Z}^r$ et son image $H \subset \mathbb{Z}^m$. Soit $A \in \mathbb{Z}^{m \times n}$ la matrice associée par rapport aux bases canoniques de $\mathbb{Z}^n$ et $\mathbb{Z}^m$. Par construction ses diviseurs élémentaires sont $e_1, \dots, e_r, 0 \dots, 0$.

Supposons que $b'_1, \dots, b'_m$ est une autre base de $\mathbb{Z}^m$ telle que $e'_1 b'_1, \dots, e'_r b'_r$ soit une base de H avec $e'_1, \dots, e'_r \geq 1$ vérifiant $e'_1 \mid \cdots \mid e'_r$. Si $A' \in \mathbb{Z}^{m \times n}$ est la matrice associée, comme avant, alors ses diviseurs élémentaires sont $e'_1, \dots, e'_r, 0 \dots, 0$. Par construction on a $A' = SAT$ avec certaines matrices de passage $S \in \mathrm{SL}_m(\mathbb{Z})$ et $T \in \mathrm{SL}_r(\mathbb{Z})$. (Leur construction détaillée est laissée en exercice.) L'unicité énoncée dans le théorème 1.15 assure que $e'_i = \pm e_i$ pour tout $i = 1, \dots, r$. □

Corollaire 2.15. *Soit G un groupe abélien libre de rang fini. Alors tout sous-groupe H de G est libre et* $\operatorname{rang} H \leq \operatorname{rang} G$. *Il existe une base $g_1, \dots, g_m$ de G et un entier r avec $0 \leq r \leq m$ et des entiers $e_1, \dots, e_r \geq 1$ vérifiant $e_1 \mid \cdots \mid e_r$ tels que $e_1 g_1, \dots, e_r g_r$ soit une base de H. La suite des entiers $e_1, \dots, e_r$ est uniquement déterminée par H, aux signes près, et on les appelle* les diviseurs élémentaires *du sous-groupe $H \subset G$.* □

Corollaire 2.16. *Soient H et H' deux sous-groupes dans G ayant les familles $(e_1, \dots, e_r)$ et $(e'_1, \dots, e'_{r'})$, respectivement, pour diviseurs élémentaires. Il existe un automorphisme $\phi\colon G \to G$ vérifiant $\phi(H) = H'$ si et seulement si $(e_1, \dots, e_r) = (e'_1, \dots, e'_{r'})$.* □

2.4. Groupes abéliens finiment engendrés. Nous concluons avec un très beau théorème, la classification des groupes abéliens finiment engendrés :

Théorème 2.17. *Soit G un groupe abélien finiment engendré. Alors il existe un isomophisme de groupes*

$$G \cong \mathbb{Z}_{e_1} \times \mathbb{Z}_{e_2} \times \cdots \times \mathbb{Z}_{e_k} \times \mathbb{Z}^r$$

où $e_1, e_2, \ldots, e_k \geq 2$ sont des entiers satisfaisant $e_1 \mid e_2 \mid \cdots \mid e_k$. Ces nombres sont uniquement déterminés par G. On appelle r le rang *de la partie libre et $e_1, e_2, \ldots, e_k$ les* diviseurs élémentaires *de G.*

DÉMONSTRATION. *Existence.* — Par hypothèse G admet une famille génératrice finie $(g_1, \ldots, g_m)$. Soit $f\colon \mathbb{Z}^m \to G$ l'homomorphisme de groupes défini par $(\lambda_1, \ldots, \lambda_m) \mapsto \lambda_1 g_1 + \cdots + \lambda_m g_m$. Par hypothèse f est surjectif, le théorème d'isomorphisme nous assure donc $G \cong \mathbb{Z}^n/K$ où $K := \ker(f) \subset \mathbb{Z}^m$ est le noyau de f. D'après le théorème 2.14 il existe une base $b_1, \ldots, b_m$ de $\mathbb{Z}^m$ de $\mathbb{Z}^m$ et des entiers $e_1, e_2, \ldots, e_k \geq 1$ vérifiant $e_1 \mid e_2 \mid \cdots \mid e_k$ tels que $e_1 b_1, \ldots, e_k b_k$ soit une base de K. Par conséquent le groupe quotient $\mathbb{Z}^m/K$ est isomorphe au groupe $\mathbb{Z}_{e_1} \times \mathbb{Z}_{e_2} \times \cdots \times \mathbb{Z}_{e_k} \times \mathbb{Z}^r$ où $r = m - k$ est le rang de la partie libre. En supprimant d'éventuels facteurs triviaux $\mathbb{Z}_1 = \mathbb{Z}/\mathbb{Z} \cong \{0\}$, nous arrivons à la forme souhaitée avec $e_1, e_2, \ldots, e_k \geq 2$.

Unicité. — Si l'on ajoute un générateur g_{m+1} à la famille génératrice $(g_1, \ldots, g_m)$, ceci élargit $\mathbb{Z}^m$ à $\mathbb{Z}^{m+1}$ mais aussi le noyau par une relation $g_{m+1} = \sum_{i=1}^m \lambda_i g_i$. Les diviseurs élémentaires ne changent que par un facteur $e = 1$ supplémentaire, ce qui ne change pas le résultat. Cet argument prouve que les diviseurs élémentaires sont indépendants du choix de la famille génératrice : si $(g_1, \ldots, g_m)$ et $(g'_1, \ldots, g'_{m'})$ sont deux familles génératrices, alors $(g_1, \ldots, g_m, g'_1, \ldots, g'_{m'})$ est aussi une famille génératrice. D'après l'argument précédent, les diviseurs élémentaires calculés à partir de ces trois familles sont les mêmes. □

Rappelons qu'un groupe G est le produit direct de sous-groupes $G_1, \ldots, G_n$, noté $G = G_1 \times \cdots \times G_n$, si et seulement si l'application $G_1 \times \cdots \times G_n \to G$ donnée par le produit $(g_1, \ldots, g_n) \mapsto g_1 \cdots g_n$ est un isomorphisme de groupes. L'algorithme de Gauss-Bézout entraîne que tout groupe abélien finiment engendré est un produit direct de sous-groupes cycliques :

Corollaire 2.18. *Soit G un groupe abélien finiment engendré. Alors il existe des éléments non triviaux $g_1, \ldots, g_n \in G$ tels que $G = \langle g_1 \rangle \times \cdots \times \langle g_n \rangle$ et les ordres $e_i = \operatorname{ord}(g_i)$ vérifient $e_1 \mid \cdots \mid e_n$. Les nombres $(e_1, \ldots, e_m)$ sont uniquement déterminés par G et caractérisent le groupe G à isomorphisme près.*

Plus explicitement : supposons que H est un autre groupe abélien tels que $H = \langle h_1 \rangle \times \cdots \times \langle h_m \rangle$ pour certains éléments non triviaux $h_1, \ldots, h_m$ dont les ordres $f_j = \operatorname{ord}(h_j)$ vérifient $f_1 \mid \cdots \mid f_m$. Alors il existe un isomorphisme $G \cong H$ si et seulement si $(e_1, \ldots, e_n) = (f_1, \ldots, f_m)$. □

Exemple 2.19. Voici la liste des groupes abéliens d'ordre ≤ 12 à isomorphismes près. Ordre 1 : $\mathbb{Z}_1$; ordre 2 : $\mathbb{Z}_2$; ordre 3 : $\mathbb{Z}_3$; ordre 4 : $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$; ordre 5 : $\mathbb{Z}_5$; ordre 6 : $\mathbb{Z}_6$; ordre 7 : $\mathbb{Z}_7$; ordre 8 : $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$; ordre 9 : $\mathbb{Z}_9$; ordre 10 : $\mathbb{Z}_{10}$; ordre 11 : $\mathbb{Z}_{11}$; ordre 12 : $\mathbb{Z}_{12}$, $\mathbb{Z}_2 \times \mathbb{Z}_6$.

Le théorème de classification assure que cette liste est complète et ne contient pas de doublons : pour tout groupe abélien G d'ordre ≤ 12 il existe un et un seul groupe dans la liste qui soit isomorphe à G.

Exercice 2.20. Les groupes $\mathbb{Z}_5^\times$ et $\mathbb{Z}_8^\times$ et $\mathbb{Z}_{12}^\times$ sont tous d'ordre 4. Pour chacun entre eux trouver le groupe isomorphe dans la liste. Même question pour le groupe $\mathbb{Z}_{13}^\times$ d'ordre 12.

Exercice 2.21. Continuer la liste des groupes abéliens jusqu'à l'ordre 32 (ou plus loin si vous voulez). Comment énumérer les groupes d'ordre p^e où p est un nombre premier ? Comment le faire dans le cas général d'ordre $p_1^{e_1} \cdots p_k^{e_k}$? À titre d'illustration, énumérer les groupes d'ordre 8000 à isomorphisme près.