Algèbre 2

Semestre d'été 2013

Université du Luxembourg

Gabor Wiese et Agnès David
gabor.wiese@uni.lu, agnes.david@uni.lu

Version du 31 mai 2013

Table des matières

Préface

Ce cours est la suite du cours Algèbre 1 enseigné au semestre d'hiver 2012/2013. Il consiste en deux parties majeures : un traitement approfondi des anneaux ; des compléments à l'algèbre linéaire d'un point de vue plus général (et plus abstrait). Ce cours sert également comme préparation au cours Algèbre 3 en semestre d'hiver 2013/2014 qui introduit la théorie de Galois qui nous permettra de démontrer la constructibilité ou inconstructibilité à la règle et au compas de certains problèmes de l'Antiquité et l'impossibilité de résoudre l'équation générale de degré au moins 5 par radicaux.

Littérature

Voici quelques références : ces livres devraient être ou devenir disponibles dans la bibliothèque au Kirchberg pendant le semestre en cours.

- Lelong-Ferrand, Arnaudiès. *Cours de mathématiques, Tome 1, Algèbre*. Dunod. Ce livre est très complet et très détaillé. On peut l'utiliser comme ouvrage de référence.
- Siegfried Bosch : *Algebra* (en allemand), Springer-Verlag. Ce livre est très complet et bien lisible.
- Serge Lang : *Algebra* (en anglais), Springer-Verlag. C'est comme une encyclopédie de l'algèbre ; on y trouve beaucoup de sujets rassemblés, écrits de façon concise.
- Siegfried Bosch. *Lineare Algebra*, Springer-Verlag.
- Jens Carsten Jantzen, Joachim Schwermer. *Algebra*.
- Christian Karpfinger, Kurt Meyberg. *Algebra : Gruppen - Ringe - Körper*, Spektrum Akademischer Verlag.
- Gerd Fischer. *Lehrbuch der Algebra : Mit lebendigen Beispielen, ausführlichen Erläuterungen und zahlreichen Bildern*, Vieweg+Teubner Verlag.
- Gerd Fischer. *Lineare Algebra : Eine Einführung für Studienanfänger*, Vieweg+Teubner Verlag.
- Gerd Fischer, Florian Quiring. *Lernbuch Lineare Algebra und Analytische Geometrie : Das Wichtigste ausführlich für das Lehramts- und Bachelorstudium*, Springer Vieweg.
- Perrin. *Cours d'algèbre*, Ellipses.
- Guin, Hausberger. *Algèbre I. Groupes, corps et théorie de Galois*, EDP Sciences.
- Fresnel. *Algèbre des matrices*, Hermann.
- Tauvel. *Algèbre*.
- Combes. *Algèbre et géométrie*.

1 Structures fondamentales

Nous commençons le cours par un rappel des structures apprises au semestre précédent ainsi que l'introduction de quelques nouvelles structures comme les homomorphismes d'anneaux et les idéaux.

Groupes, anneaux, corps, modules, espaces vectoriels

Définition 1.1. *Un ensemble G avec un élément $e \in G$ et muni d'une application (*loi interne, loi de groupe*)*

$$* : G \times G \to G$$

est appelé un groupe (group, Gruppe) *si*

Associativité : $\forall\, g_1, g_2, g_3 \in G :\ (g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$,

Élément neutre : $\forall\, g \in G : e * g = g * e = g$ *et*

Existence d'inverse : $\forall\, g \in G\ \exists\, h \in G : h * g = g * h = e$.

Données : $(G, *, e)$.
Un groupe $(G, *, e)$ *est appelé* commutatif *ou* abélien *si*

Commutativité : $\forall\, g_1, g_2 \in G : g_1 * g_2 = g_2 * g_1$.

Exemple 1.2. – $(\mathbb{Z}, +, 0)$ *est un groupe abélien.*
– *Le groupe symétrique* $(S_n, \circ, (1))$ *est un groupe non-abélien dès que* $n \geq 3$ *(voir Algèbre 1).*
– *On note* $\mathrm{Mat}_n(\mathbb{R})$ *les matrices réelles d'ordre* n *(pour* $n \in \mathbb{N}$*). Alors,* $(\mathrm{Mat}_n(\mathbb{R}), +, \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix})$ *est un groupe abélien. On écrira aussi* 0 *pour l'élément neutre de ce groupe.*
– *On note*

$$\mathrm{GL}_n(\mathbb{R}) := \{M \in \mathrm{Mat}_n(\mathbb{R}) \mid M \text{ est inversible } \} = \{M \in \mathrm{Mat}_n(\mathbb{R}) \mid \det(M) \neq 0\},$$

appelé le groupe général linéaire. *Alors,* $(\mathrm{GL}_n(\mathbb{R}), \circ, \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix})$ *est un groupe où* $\circ$ *est la multiplication des matrices (voir le cours d'algèbre linéaire 1). On écrira aussi* 1 *pour l'élément neutre de ce groupe. Ce groupe n'est pas abélien dès que* $n > 1$*. Trouvez vous-même un exemple de matrices qui ne commutent pas !*

Définition 1.3. *Un ensemble A avec deux éléments (pas nécessairement distincts) muni de deux applications*

$$+_A : A \times A \to A, \quad \text{et} \quad \cdot_A : A \times A \to A$$

est appelé anneau (Ring) *si*

Groupe additif : $(A, +_A, 0_A)$ *est un groupe abélien,*

Associativité : $\forall\, a, b, c \in A :\ (a \cdot b) \cdot c = a \cdot (b \cdot c)$,

Élément neutre : $\forall\, a \in A : 1_A \cdot a = a \cdot 1_A = a$ *et*

Distributivité : *Pour tous* $a, b, c \in A$ *:*

$$a \cdot_A (b +_A c) = (a \cdot_A b) +_A (a \cdot_A c)$$

et

$$(a +_A b) \cdot_A c = (a \cdot_A c) +_A (b \cdot_A c).$$

Données : $(A, +, \cdot, 0_A, 1_A)$ *(nous écrirons* $0 = 0_A$ *et* $1 = 1_A$ *dans la suite).*
Un anneau $(A, +, \cdot, 0_A, 1_A)$ *est appelé* commutatif *si*

Commutativité : $\forall\, a, b \in A :\ a \cdot b = b \cdot a$.

Dans la littérature ce que nous appelons *anneau* est souvent appelé *anneau unitaire* pour souligner l'existence d'un élément neutre pour la multiplication. La plupart des anneaux dans ce cours seront commutatifs.

Exemple 1.4. – $(\mathbb{Z}, +, \cdot, 0, 1)$ *est un anneau commutatif.*
– $(\mathrm{Mat}_n(\mathbb{R}), +, \circ, \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix})$ *est un anneau. Il n'est pas commutatif dès que* $n \geq 2$.

Définition-Lemme 1.5 (Algèbre 1, 5.8)**.** *Soit* $(A, +, \cdot, 0, 1)$ *un anneau. Un élément* $u \in A$ *est appelé* unité *s'il existe* $v \in A$ *tel que* $uv = vu = 1$*. Une unité est donc un élément inversible dans le monoïde* $(A, \cdot, 1)$.
L'ensemble des unités de A *est noté* $A^\times$*.* $(A^\times, \cdot, 1)$ *est un groupe (abélien si l'anneau est commutatif). Il s'appelle* groupe des unités de A.

Définition 1.6. *Soit* $(A, +, \cdot, 0, 1)$ *un anneau (commutatif). On l'appelle* corps (commutatif) *si*
– *tout* $0 \neq a \in A$ *est une unité pour la multiplication (c'est-à-dire,* $A^\times = A \setminus \{0\}$*) et*
– $0 \neq 1$.

Remarque 1.7. *Traductions :*
– *Anglais :* field *veut dire « corps commutatif ».*
– *Anglais :* skew field *veut dire « corps non-commutatif ».*
– *Allemand :* Körper *veut dire « corps commutatif ».*
– *Allemand :* Schiefkörper *veut dire « corps non-commutatif ».*
– *Néerlandais :* lichaam *veut dire « corps commutatif ».*
– *Flamand :* veld *veut dire « corps commutatif ».*

Donc, dans les langues différentes du français il semble que tout corps est automatiquement commutatif.
Dans ce cours nous supposons aussi que tout corps est commutatif. *Donc nous utilisons le mot « corps » pour signifier « corps commutatif ».*

Exemple 1.8. – $(\mathbb{Q}, +, \cdot, 0, 1)$ *est un corps.*
– $(\mathbb{R}, +, \cdot, 0, 1)$ *est un corps.*
– $(\mathbb{Z}, +, \cdot, 0, 1)$ *n'est pas un corps.*
– *Soit* p *un nombre premier.* $\mathbb{F}_p := (\mathbb{Z}/p\mathbb{Z}, +, \cdot, \overline{0}, \overline{1})$ *est un corps fini à* p *éléments (voir Algèbre 1, 5.32).*

Définition 1.9. *Soit $K = (K, +, \cdot, 0, 1)$ un corps (commutatif !). Un groupe abélien $(V, +, 0)$ muni d'une application (« multiplication scalaire »)*

$$. : K \times V \to V$$

est appelé K-espace vectoriel (K-vector space, K-Vektorraum) *si*
– $\forall\, v \in V :\ 1.v = v$,
– $\forall\, a \in K, \forall\, v, w \in V :\ a.(v + w) = a.v + a.w$,
– $\forall\, a, b \in K, \forall\, v \in V :\ (a + b).v = a.v + b.v$ *et*
– $\forall\, a, b \in K, \forall\, v \in V :\ (a \cdot b).v = a.(b.v)$.
Données : $(V, +, ., 0)$.

Remarque 1.10. *On peut faire la même définition avec un anneau commutatif au lieu d'un corps. Dans ce cas on parle d'un* A-module *ou plus précisément d'un* A-module à gauche *. On ne les traitera pas dans ce cours, mais ils joueront un rôle important dans le cours « Commutative Algebra » dans le Master of Mathematics.*

Exemple 1.11. – $(\mathbb{R}^n, +, ., \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix})$ *est un* $\mathbb{R}$*-espace vectoriel. Nous écrivons aussi* 0 *pour le vecteur zéro.*
– $(\mathbb{Q}^n, +, ., \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix})$ *est un* $\mathbb{Q}$*-espace vectoriel.*
– $(\mathrm{Mat}_n(\mathbb{R}), +, ., \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix})$ *est un* $\mathbb{R}$*-espace vectoriel.*

Homomorphismes

Les homomorphismes sont des applications qui préservent toutes les structures. On connaît déjà les homomorphismes de groupes : ils préservent la loi de groupe et l'élément neutre. On introduira les homomorphismes d'anneaux (qui préservent les deux opérations $+$, $\cdot$, ainsi que les éléments neutres) et les homomorphismes d'espaces vectoriels (qui préservent l'addition, la multiplication scalaire et l'élément neutre).

Définition 1.12. *Soient $(G, \star, e)$ et $(H, \circ, \epsilon)$ deux groupes. Une application*

$$\varphi : G \to H$$

est appelée (homo)morphisme de groupes *si pour tout $g_1, g_2 \in G$ on a*

$$\varphi(g_1 \star g_2) = \varphi(g_1) \circ \varphi(g_2).$$

Exemple 1.13. – $\varphi : \mathbb{Z} \to \mathbb{Z}$, $n \mapsto 2n$, *définit un homomorphisme de groupes de $(\mathbb{Z}, +, 0)$ dans lui-même.*
– *Le déterminant* $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$ *définit un homomorphisme de groupes de* $\mathrm{GL}_n(\mathbb{R})$ *dans le groupe des unités de* $\mathbb{R}$ *(qui est égal à* $\mathbb{R} \setminus \{0\}$ *car* $\mathbb{R}$ *est un corps).*
Si la loi de groupe ainsi que l'élément neutre sont clairs, on les supprime (comme fait dans cet exemple).

– *Pour des propriétés importantes voir Algèbre 1, 7.20.*

Définition 1.14. *Soient* $(A, +, \cdot, 0, 1)$ *et* $(A', +', \cdot', 0', 1')$ *deux anneaux. Une application*

$$\varphi : A \to A'$$

est appelée (homo)morphisme d'anneaux *si*
– φ *est un homomorphisme de groupes de* $(A, +, 0)$ *dans* $(A', +', 0')$*, c'est-à-dire*
$\forall\, a, b \in A :\ \varphi(a + b) = \varphi(a) +' \varphi(b)$,
– $\forall\, a, b \in A :\ \varphi(a \cdot b) = \varphi(a) \cdot' \varphi(b)$ *et*
– $\varphi(1) = 1'$.
Si A *et* A' *sont des corps, on parle aussi d'un* homomorphisme de corps.

Remarque 1.15. *Pour un homomorphisme de groupes c'est une conséquence de la définition (comme on l'a vu) que l'élément neutre est envoyé sur l'élément neutre. Par contre, pour un homomorphisme d'anneaux,* $\varphi(1) = 1'$ *n'est en général pas une conséquence des deux premières propriétés (par exemple, l'homomorphisme qui envoie tout élément sur* 0 *vérifie les deux premières propriétés).*

Exemple 1.16. – *L'inclusion* $\varphi : \mathbb{Z} \to \mathbb{Q}$, $n \mapsto \frac{n}{1}$ *est un homomorphisme d'anneaux.*
– *L'inclusion* $\varphi : \mathbb{R} \to \mathrm{Mat}_n(\mathbb{R})$, $a \mapsto \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & a & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a \end{pmatrix}$ *est un homomorphisme d'anneaux (Exercice sur la feuille 2).*
– *Soit* $n \in \mathbb{N}_{>0}$. *L'application* $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $a \mapsto \overline{a} = a + n\mathbb{Z}$, *est un homomorphisme d'anneaux (Exercice sur la feuille 1).*

Définition 1.17. *Soient* A *et* B *des anneaux et* $\varphi : A \to B$ *un homomorphisme d'anneaux. On suppose* A *commutatif. Alors, on appelle* (B, φ) *une* A-algèbre *si pour tout* $a \in A$ *et tout* $b \in B$ *on a* $\varphi(a) \cdot b = b \cdot \varphi(a)$.

Ce que nous appelons « algèbre » s'appelle souvent plus précisement « algèbre associative (unitaire) ».

Exemple 1.18. *Soient* $n \in \mathbb{N}_{>0}$, $(K, +, \cdot, 0, 1)$ *un corps (commutatif !) et* $\varphi : K \to \mathrm{Mat}_n(K)$, $a \mapsto \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & a & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a \end{pmatrix}$. *Alors,* $(\mathrm{Mat}_n(K), \varphi)$ *est une* K*-algèbre (Exercice sur la feuille 2).*

Définition 1.19. *Soient* K *un corps et* V, W *deux* K*-espaces vectoriels. Une application* $\varphi : V \to W$ *est appelée* homomorphisme de K-espaces vectoriels *ou* application K-linéaire *si*
– φ *est un homomorphisme de groupes de* V *dans* W*, c'est-à-dire*
$\forall\, v_1, v_2 \in V :\ \varphi(v_1 + v_2) = \varphi(v_1) + \varphi(v_2)$ *et*
– $\forall\, a \in K, \forall\, v \in V :\ \varphi(a.v) = a.\varphi(v)$.

Exemple 1.20. *Soient* K *un corps et* $V = K^n$, $W = K^m$ *avec* $n, m \in \mathbb{N}_{>0}$. *Alors, toute matrice* $D = \begin{pmatrix} d_{1,1} & d_{1,2} & \cdots & d_{1,n} \\ d_{2,1} & d_{2,2} & \cdots & d_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ d_{m,1} & d_{m,2} & \cdots & d_{m,n} \end{pmatrix} \in \mathrm{Mat}_{m \times n}(K)$ *définit une application* K*-linéaire*

$$V \to W, \quad \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} d_{1,1} & d_{1,2} & \cdots & d_{1,n} \\ d_{2,1} & d_{2,2} & \cdots & d_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ d_{m,1} & d_{m,2} & \cdots & d_{m,n} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix},$$

donnée par la multiplication de la matrice et du vecteur.
Un théorème important d'algèbre linéaire (que nous allons (re)démontrer dans la deuxième partie du cours) dit que – après choix de bases – toute application linéaire est uniquement donnée par une matrice.

Définition 1.21. *Si un homomorphisme (de groupes, d'anneaux ou d'espaces vectoriels) est bijectif, on parle d'un* isomorphisme.
Dans la littérature on trouve aussi les mots monomorphisme *pour un homomorphisme injectif, et* épimorphisme *pour un homomorphisme surjectif.*

Sous-objets

Définition 1.22. *Soient $(G, \star, e)$ un groupe et $H \subseteq G$ un sous-ensemble. H est appelé* sous-groupe de G *(notation $H \leq G$) si*
– $e \in H$,
– *pour tous $a, b \in H$ on a $a \star b \in H$ (donc, $\star$ se restreint en une application $H \times H \to H$), et*
– *pour tout $a \in H$, l'inverse $a^{-1} \in H$.*
Un sous-groupe $H \leq G$ est appelé normal *(notation : $H \trianglelefteq G$) si*

$$\forall\, h \in H, \forall\, g \in G :\ g^{-1}hg \in H.$$

Exemple 1.23. – *Si G est abélien, tout sous-groupe $H \leq G$ est normal (Algèbre 1, 8.8).*
– *Soit $\varphi : G_1 \to G_2$ un homomorphisme de groupes. Alors, le* noyau de φ

$$\ker(\varphi) := \{g \in G_1 \mid \varphi(g) = 1_{G_2}\} \trianglelefteq G_1$$

(où 1_{G_2} est l'élément neutre de G_2) est un sous-groupe normal de G_1 et l'image de φ

$$\mathrm{im}(\varphi) := \{g \in G_2 \mid \exists g_1 \in G_1 : \varphi(g_1) = g\} \leq G_2$$

est un sous-groupe (pas nécéssairement normal) de G_2 (Algèbre 1, 7.20, 8.10).

Définition 1.24. *Soit A un anneau commutatif. Un sous-ensemble $B \subseteq A$ est appelé* sous-anneau de A *si*
– *$(B, +, 0)$ est un sous-groupe de $(A, +, 0)$ (alors, pour tout $b_1, b_2 \in B$, on a $b_1 - b_2 \in B$),*
– *pour tout $b_1, b_2 \in B$ on a $b_1 \cdot b_2 \in B$ et*
– $1 \in B$.
Un sous-ensemble $I \subseteq A$ est appelé idéal de A *(notation : $I \trianglelefteq A$) si*
– *$(I, +, 0)$ est un sous-groupe de $(A, +, 0)$ (alors, pour tout $i_1, i_2 \in I$, on a $i_1 - i_2 \in I$) et*
– *pour tout $i \in I$ et tout $a \in A$ on a $a \cdot i \in I$.*

Remarque 1.25. *Si A n'est pas commutatif, la définition que nous avons donnée est celle d'un* idéal à gauche. *Il est évident comment définir les idéaux à droite (remplacer $a \cdot i \in A$ par $i \cdot a \in A$ dans la dernière condition) ; on a aussi la notion d'idéal bilatère. Dans ce cours nous allons utiliser uniquement les idéaux pour les anneaux commutatifs, comme dans la définition précédente.*

Exemple 1.26. *Soit $\varphi : A_1 \to A_2$ un homomorphisme d'anneaux. Alors, le* noyau de φ

$$\ker(\varphi) := \{a \in A_1 \mid \varphi(a) = 0\} \trianglelefteq A_1$$

est un idéal de A_1 et l'image de φ

$$\mathrm{im}(\varphi) := \{a \in A_2 \mid \exists a_1 \in A_1 : \varphi(a_1) = a\} \subseteq A_2$$

est un sous-anneau (pas nécéssairement un idéal) de A_2 (Exercice sur la feuille 1).

Définition 1.27. *Soient K un corps et V un K-espace vectoriel. Un sous-ensemble $W \subseteq V$ est appelé* sous-K-espace (vectoriel) de V *(notation : $W \leq V$) si*
– *$(W, +, 0)$ est un sous-groupe de $(V, +, 0)$ (alors, pour tout $w_1, w_2 \in W$, on a $w_1 - w_2 \in W$),*
– *pour tout $a \in K$ et tout $w \in W$ on a $a.w \in W$.*

Exemple 1.28. – *$V = \mathbb{Q}^2$. Alors, $W := \{\binom{a}{a} \mid a \in \mathbb{Q}\}$ est un sous-$\mathbb{Q}$-espace de $\mathbb{Q}^2$.*
– *Soient K un corps et $\varphi : V_1 \to V_2$ un homomorphisme de K-espaces vectoriels. Alors, le* noyau de φ

$$\ker(\varphi) := \{v \in V_1 \mid \varphi(v) = 0\} \leq V_1$$

est un sous-K-espace de V_1 et l'image de φ

$$\mathrm{im}(\varphi) := \{v \in V_2 \mid \exists v_1 \in V_1 : \varphi(v_1) = v\} \subseteq V_2$$

est un sous-K-espace de V_2 (Exercice sur la feuille 1).

2 Quotients

Dans cette section nous traitons les quotients pour les différentes structures introduites/rappelées dans la section précédente. C'est-à-dire que nous commençons par rappeler la construction dans le cas des groupes, puis on passera aux anneaux et finalement on traitera les espaces vectoriels.

Quotients de groupes

On rappelle d'abord les conventions sur les groupes introduites au dernier semestre :
– Nous ne devons jamais oublier qu'un groupe est un triplet $(G, \circ, e)$ où G est l'ensemble des éléments de G, $\circ$ désigne la loi de groupe (loi interne) et e est l'élément neutre. On peut évidemment choisir n'importe quel symbole. Des symboles souvent utilisés pour la loi de groupe sont $\cdot$, $+$, $\times$, $*$, $\circ$, mais on pourrait aussi choisir `BelleMultiplication`.
– Souvent on n'a pas envie d'écrire le triplet et on n'écrit que $(G, \circ)$ ou bien « G pour la loi $\circ$ ». Dans ce cas, on écrit souvent e_G ou juste e pour l'élément neutre. Normalement, une confusion est impossible car il n'y a qu'un seul élément neutre dans le groupe (comme on l'a démontré en Algèbre 1).
– Si la loi de groupe est un symbole qui rappelle la multiplication comme $\cdot$, $\times$, $*$, $\circ$, $\otimes$, on écrit souvent 1 pour l'élément neutre ; dans ce cas on note g^{-1} l'inverse d'un élément g du groupe. Par contre, si le symbole rappelle l'addition comme $+$, $\oplus$, l'élément neutre s'écrit 0 (au lieu de 1, car l'égalité $1 + 1 = 1$ serait trop bizarre) et $-g$ est l'inverse de g. La notation additive est en général réservée aux groupes commutatifs.

– Si nous écrivons « Soit G un groupe » sans spécifier ni la loi de groupe ni l'élément neutre, on utilise un symbole multiplicatif comme $\cdot$, $\times$ (selon votre et notre goût) pour la loi de groupe et 1 pour l'élément neutre.

Soit $n \in \mathbb{N}_{\geq 1}$. On considère le groupe $G = (\mathbb{Z}, +, 0)$ et son sous-groupe $H = n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$ (qui est normal, ce qui va être implicitement utilisé plus bas). Par la division euclidienne tout $m \in \mathbb{Z}$ s'écrit de façon unique comme

$$m = qn + r$$

avec $q \in \mathbb{Z}$ et un « reste » $0 \leq r \leq n-1$. Pour $a, b \in \mathbb{Z}$ les assertions suivantes sont équivalentes :

(i) a et b ont le même reste dans la division euclidienne par n ;

(ii) $a \in b + n\mathbb{Z} = \{b + nm \mid m \in \mathbb{Z}\}$;

(iii) $a - b \in n\mathbb{Z}$;

(iv) $n \mid (a - b)$;

(v) $a \equiv b \mod n$.

La dernière équivalence est une définition (voir Algèbre 1). Si $0 \leq r \leq n-1$, l'ensemble $r + n\mathbb{Z}$ est l'ensemble de tous les entiers relatifs qui ont r comme reste dans la division euclidienne par n. Comme tout entier m a un entier entre 0 et $n-1$ comme reste, nous avons la réunion disjointe

$$\mathbb{Z} = \bigsqcup_{r=0}^{n-1} (r + n\mathbb{Z}).$$

Dans le contexte d'un groupe général, la généralisation abstraite de ce qui précède est contenue dans la définition-lemme suivante, déjà traitée en Algèbre 1.

Définition-Lemme 2.1. *Soit G un groupe et $H \leq G$ un sous-groupe. La relation définie par*

$$g_1 \sim_H g_2 \quad :\Leftrightarrow \quad g_1^{-1} \cdot g_2 \in H$$

est une relation d'équivalence.
Les classes d'équivalence sont de la forme

$$gH = \{g \cdot h \mid h \in H\}$$

et elles s'appellent classes à gauche de G suivant H. *L'ensemble de ces classes est noté G/H.*
Donc, on a
– $G = \bigsqcup_{gH \in G/H} gH$,
– $g_1H \cap g_2H = \begin{cases} \emptyset & \text{si } g_1^{-1}g_2 \notin H, \\ g_1H = g_2H & \text{si } g_1^{-1}g_2 \in H. \end{cases}$
Un élément $g_2 \in g_1H$ est appelé un représentant *de la classe g_1H. On a alors $g_1H = g_2H$.*

Démonstration. La vérification que c'est une relation d'équivalence était un exercice en Algèbre 1. Le reste est une conséquence valable pour toutes les relations d'équivalence. □

Donc, $r + n\mathbb{Z}$ est la classe à gauche de r dans $\mathbb{Z}$ suivant $n\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble de ces classes. Nous continuons en rappelant la structure de groupe de $\mathbb{Z}/n\mathbb{Z}$.
Observation fondamentale : Soient $a, a', b, b' \in \mathbb{Z}$ tels que

$$a \equiv a' \mod n \quad \text{et} \quad b \equiv b' \mod n.$$

Alors,

$$a + b \equiv a' + b' \mod n.$$

(Bien que cette observation soit si fondamentale pour ce qui suit, la preuve en est très facile : comme $n \mid (a' - a)$ et $n \mid (b' - b)$, il existe $c, d \in \mathbb{Z}$ tels que $a' = a + cn$ et $b' = b + dn$; donc $a' + b' = a + b + (c + d)n$ et n divise $(a' + b') - (a + b)$.) Un petit exemple :

$$(3 \equiv 23 \mod 10 \quad \text{et} \quad 9 \equiv -51 \mod 10) \quad \Rightarrow \quad 12 \equiv -28 \equiv 2 \mod 10.$$

Nous écrivons aussi $\overline{a}$ pour la classe à gauche $a + n\mathbb{Z}$. Le but est de définir une loi de groupe sur l'ensemble des classes à gauche ; pour que la distinction avec l'addition sur $\mathbb{Z}$ soit bien claire, nous notons la nouvelle loi de groupe par $\oplus$ pour l'instant (plus tard on va seulement écrire $+$) :

$$\oplus : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}.$$

Il faut donc définir ce qu'on veut comprendre par la somme de $\overline{a} = (a + n\mathbb{Z})$ et $\overline{b} = (b + n\mathbb{Z})$; il ne s'agit pas de la somme de deux entiers, mais d'une somme de deux *ensembles d'entiers* ! Comme $\oplus$ doit être une application, nous avons besoin d'une règle qui à deux classes données associe une troisième classe. C'est ici que l'observation fondamentale intervient ; elle donne :

> Soient a et a' deux représentants de la même classe, c'est-à-dire $a' + n\mathbb{Z} = a + n\mathbb{Z}$;
> soient b et b' aussi dans la même classe : $b' + n\mathbb{Z} = b + n\mathbb{Z}$.
> Alors $a' + b'$ et $a + b$ représentent aussi la même classe : $(a' + b') + n\mathbb{Z} = (a + b) + n\mathbb{Z}$.

Cela veut dire : *la classe $(a + b) + n\mathbb{Z}$ ne dépend que de la classe de a et de la classe de b.* Ceci nous donne la définition recherchée :

$$\overline{a} \oplus \overline{b} = (a + n\mathbb{Z}) \oplus (b + n\mathbb{Z}) := (a + b) + n\mathbb{Z} = \overline{(a + b)}.$$

Voici la version abstraite de ce qui précède (déjà traité, Algèbre 1, Prop. 8.12).

Proposition 2.2. *Soit $(G, \cdot, 1)$ un groupe et $N \trianglelefteq G$ un sous-groupe normal.*

(a) Soient $g_1N = g_2N, h_1N = h_2N \in G/N$ des classes de G suivant N. Alors, $(g_1h_1)N = (g_2h_2)N$.

(b) (a) permet de définir l'application

$$\star : G/N \times G/N \to G/N, \quad (gN, hN) \mapsto gN \star hN := (gh)N.$$

(c) $(G/N, \star, N)$ est un groupe, appelé quotient de G par N.

(d) L'application

$$\pi : G \to G/N, \quad g \mapsto gN$$

est un homomorphisme de groupes surjectif, appelé projection naturelle. *On a* $\ker(\pi) = N$.

Rappelons une proposition importante (Algèbre 1, Prop. 8.14) :

Proposition 2.3. *Soit G un groupe et $N \trianglelefteq G$ un sous-groupe normal et $\pi : G \to G/N$ la projection naturelle.*

(a) L'application

$$\Phi : \{\text{sous-groupes de } G/N\} \longrightarrow \{\text{sous-groupes de } G \text{ qui contiennent } N\},$$

donnée par $H \mapsto \pi^{-1}(H)$ est bijective. L'inverse de Φ est $U \mapsto \pi(U)$.

(b) Soient $H_1, H_2 \leq G/N$ deux sous-groupes. Alors

$$H_1 \subseteq H_2 \quad \Leftrightarrow \quad \Phi(H_1) \subseteq \Phi(H_2).$$

(c) Soit $H \leq G/N$ un sous-groupe. Alors

$$H \trianglelefteq G/N \quad \Leftrightarrow \quad \Phi(H) \trianglelefteq G.$$

Nous rappelons aussi le premier théorème d'isomorphisme (Algèbre 1, Prop. 8.15) :

Théorème 2.4 (1er théorème d'isomorphisme/Homomorphiesatz)**.** *Soit $\varphi : G \to H$ un homomorphisme de groupe. Soit $N := \ker(\varphi)$ son noyau.*

(a) Pour tout $g \in G$ et tout $n \in N$ on a $\varphi(gn) = \varphi(g)$. Donc pour tout $g_1, g_2 \in gN$ on a $\varphi(g_1) = \varphi(g_2)$. Donc l'image $\varphi(g)$ ne dépend que de la classe gN de g suivant N.

(b) (a) nous permet de définir l'application

$$\overline{\varphi} : G/N \to H, \quad gN \mapsto \overline{\varphi}(gN) := \varphi(g).$$

C'est un homomorphisme injectif de groupes. Donc $\overline{\varphi} : G/N \to \mathrm{im}(\varphi)$ est un isomorphisme de groupes.

Quotients d'anneaux

On continue l'exemple de $\mathbb{Z}/n\mathbb{Z}$. On veut maintenant le munir d'une structure d'anneau. Comme ci-dessus, nous avons une **observation fondamentale** à faire : soient $a, a', b, b' \in \mathbb{Z}$ tels que

$$a \equiv a' \mod n \quad \text{et} \quad b \equiv b' \mod n,$$

alors,

$$a \cdot b \equiv a' \cdot b' \mod n.$$

(La preuve en est aussi très facile : comme $n \mid (a' - a)$ et $n \mid (b' - b)$, il existe $c, d \in \mathbb{Z}$ tels que $a' = a + cn$ et $b' = b + dn$; donc

$$a'b' = (a + cn)(b + dn) = ab + n(ad + bc + cdn) \text{ ;}$$

ainsi, n divise $a'b' - ab$.) Un petit exemple :

$$(3 \equiv 13 \mod 10 \quad \text{et} \quad 6 \equiv -4 \mod 10) \quad \Rightarrow \quad 18 \equiv -52 \equiv 8 \mod 10.$$

Le but maintenant est de définir une multiplication sur l'ensemble des classes à gauche ; pour que la distinction avec la multiplication de $\mathbb{Z}$ soit bien claire, nous notons la nouvelle loi par $\otimes$ pour l'instant (plus tard on va seulement écrire $\cdot$) :

$$\otimes : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}.$$

Il faut donc définir ce qu'on veut comprendre par le produit de $\overline{a} = (a+n\mathbb{Z})$ et $\overline{b} = (b+n\mathbb{Z})$; comme pour le cas de $\oplus$ il ne s'agit pas d'un produit de deux entiers, mais d'un produit de deux *ensembles d'entiers* ! Comme $\otimes$ doit être une application, nous avons besoin d'une règle qui à deux classes données associe une troisième classe. On le fait comme avant en utilisant l'observation fondamentale qui nous donne :

> Soient a et a' deux représentants de la même classe, c'est-à-dire $a' + n\mathbb{Z} = a + n\mathbb{Z}$; soient b et b' aussi dans la même classe : $b' + n\mathbb{Z} = b + n\mathbb{Z}$.
>
> Alors $a'b'$ et ab représentent aussi la même classe : $a'b' + n\mathbb{Z} = ab + n\mathbb{Z}$.

Cela veut dire : *la classe $ab + n\mathbb{Z}$ ne dépend que de la classe de a et de la classe de b.* Ceci nous permet de faire la définition recherchée :

$$\overline{a} \otimes \overline{b} = (a + n\mathbb{Z}) \otimes (b + n\mathbb{Z}) := ab + n\mathbb{Z} = \overline{ab}.$$

Nous passons maintenant au cas d'un anneau commutatif général $(A, +, \cdot, 0, 1)$ pour généraliser ce qui précède. Soit I un sous-groupe de $(A, +, 0)$. Nous allons maintenant voir que I doit être un idéal pour pouvoir construire le quotient A/I, mais nous ne le supposons pas encore.
Comme $(A, +, 0)$ est un groupe abélien, le sous-groupe $I \leq A$ est normal. On considère le groupe quotient $(A/I, \oplus, 0 + I)$ qui résulte de la proposition 2.2 et notre but est de définir une multiplication

$$\otimes : A/I \times A/I \to A/I$$

telle que $(A/I, \oplus, \otimes, 0+I, 1+I)$ est un anneau. Pour ceci on veut imiter l'observation fondamentale. Soient $a, a', b, b' \in A$ tels que

$$a' - a \in I \quad \text{et} \quad b' - b \in I.$$

Il existe donc $i, j \in I$ tels que $a' = a + i$ et $b' = b + j$; donc

$$a'b' = (a + i)(b + j) = ab + aj + bi + ij.$$

Nous voulons $a'b' - ab \in I$. Ceci est clairement satisfait si I est un idéal ! Donc supposons cela. On l'applique comme avant :

> Soient a et a' deux représentants de la même classe, c'est-à-dire $a' + I = a + I$; soient b et b' aussi dans la même classe : $b' + I = b + I$.
>
> Alors $a'b'$ et ab représentent aussi la même classe : $a'b' + I = ab + I$.

Cela veut dire : *la classe $ab + I$ ne dépend que de la classe de a et de la classe de b.* Ceci nous permet de faire la définition recherchée :

$$(a + I) \otimes (b + I) := ab + I.$$

Plus précisément nous avons la proposition suivante :

Proposition 2.5. *Soient $(A, +, \cdot, 0, 1)$ un anneau commutatif et $I \trianglelefteq A$ un idéal. Avec les définitions ci-dessus nous avons :*

(a) $(A/I, \oplus, \otimes, 0 + I, 1 + I)$ *est un anneau commutatif, appelé* (anneau) quotient de A par I.

(b) L'application

$$\pi : A \to A/I, \quad a \mapsto a + I$$

est un homomorphisme d'anneaux surjectif, appelé projection naturelle. *On a* $\ker(\pi) = I$.

Démonstration. Exercice. Vous pouvez (et devrez) utiliser que nous savons déjà par la proposition 2.5 que $(A/I, \oplus, 0 + I)$ est un groupe abélien. □

Exemple 2.6. *Le plus important exemple que nous connaissons pour l'instant est $\mathbb{Z}/n\mathbb{Z}$; noter que $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$!*

Remarque 2.7. *Si l'anneau n'est pas commutatif, on peut quand-même construire un quotient si l'idéal I est bilatère. On ne le fera pas dans ce cours.*

Proposition 2.8. *Soit A un anneau et $I \trianglelefteq A$ un idéal et $\pi : A \to A/I$ la projection naturelle. Alors, l'application*

$$\Phi : \{\text{idéaux de } A/I\} \longrightarrow \{\text{idéaux de } A \text{ qui contiennent } I\},$$

donnée par $J \mapsto \pi^{-1}(J)$ est bijective. L'inverse de Φ est $K \mapsto \pi(K)$.

Démonstration. Exercice. On peut utiliser les résultats de la proposition 2.3. □

Théorème 2.9 (1er théorème d'isomorphisme/Homomorphiesatz)**.** *Soit $\varphi : A \to B$ un homomorphisme d'anneaux commutatifs. Soit $N := \ker(\varphi)$ son noyau. L'application*

$$\overline{\varphi} : A/N \to B, \quad a + N \mapsto \overline{\varphi}(a + N) := \varphi(a)$$

provenant du cas des groupes (théorème 2.4) est un isomorphisme d'anneaux.

Démonstration. On sait déjà que $\overline{\varphi}$ est un isomorphisme de groupes. Donc il suffit de démontrer que c'est un homomorphisme d'anneaux :
– $\overline{\varphi}(1 + N) = \varphi(1) = 1$.
– $\overline{\varphi}((a + N) \otimes (b + N)) = \overline{\varphi}(a \cdot b + N) = \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) = \overline{\varphi}(a + N) \cdot \overline{\varphi}(b + N)$.
□

Quotients d'espaces vectoriels

Proposition 2.10. *Soient K un corps, $(V, +, ., 0)$ un K-espace vectoriel, $W \leq V$ un sous-K-espace vectoriel et $(V/W, +, W)$ le quotient du groupe $(V, +, 0)$ par son sous-groupe W.*

(a) Alors pour tout $a \in K$ et tout $v \in V$, la classe $a.v + W$ ne dépend que de la classe $v + W$. Donc, on peut définir l'application

$$. : K \times V/W \to V/W, \quad (a, v + W) \mapsto a.v + W.$$

(b) $(V/W, +, ., 0 + W)$ *est un K-espace vectoriel, appelé* quotient de V par W.

(c) L'application

$$\pi : V \to V/W, \quad v \mapsto v + W$$

est K-linéaire et surjective de noyau $\ker(\pi) = W$ *; elle est appelée* projection naturelle.

Démonstration. Exercice sur la feuille 3. □

Théorème 2.11 (1er théorème d'isomorphisme/Homomorphiesatz)**.** *Soient K un corps et $\varphi : V \to W$ un homomorphisme d'espaces vectoriels. Soit $N := \ker(\varphi)$ son noyau. L'application*

$$\overline{\varphi} : V/N \to W, \quad v + N \mapsto \overline{\varphi}(v + N) := \varphi(v)$$

provenant du cas des groupes (théorème 2.4) est un isomorphisme d'espaces vectoriels.

Démonstration. On sait déjà que $\overline{\varphi}$ est un isomorphisme de groupes. Donc il suffit de démontrer que la multiplication scalaire est respectée :

$$\overline{\varphi}(a.(v + N)) = \overline{\varphi}(a.v + N) = \varphi(a.v) = a.\varphi(v) = a.\overline{\varphi}(v + N)$$

pour tout $a \in K$ et tout $v \in V$. □

Plus de théorèmes d'isomorphisme pour les groupes

Lemme 2.12. *Soient G un groupe, $H \leq G$ un sous-groupe et $N \leq G$ un sous-groupe normal. Soit $HN := \{hn \mid h \in H, n \in N\}$. Alors :*

(a) $H \cap N$ est un sous-groupe normal de H.

(b) $HN = NH := \{nh \mid h \in H, n \in N\}$

(c) HN est un sous-groupe de G.

(d) N est un sous-groupe normal de HN.

(e) Si H est aussi un sous-groupe normal de G, alors HN est un sous-groupe normal de G.

Démonstration. C'était un exercice sur la feuille 13 d'Algèbre 1. □

Proposition 2.13 (Deuxième théorème d'isomorphisme)**.** *Soient G un groupe, $H \leq G$ un sous-groupe et $N \leq G$ un sous-groupe normal. Alors, l'homomorphisme naturel de groupes*

$$\varphi : H \to HN \to HN/N, \quad h \mapsto hN$$

« induit » (par le théorème d'isomorphisme 2.4) l'isomorphisme de groupes

$$\overline{\varphi} : H/(H \cap N) \to HN/N, \quad h(H \cap N) \mapsto hN.$$

Démonstration. Noter d'abord que le lemme 2.12 nous assure que tout est bien défini. L'homomorphisme φ est visiblement surjectif et son noyau est composé des éléments $h \in H$ tels que $hN = N$, donc $h \in H \cap N$, montrant $\ker(\varphi) = H \cap N$. L'existence de $\overline{\varphi}$ résulte donc d'une application directe du théorème d'isomorphisme 2.4. □

Proposition 2.14 (Troisième théorème d'isomorphisme)**.** *Soient G un groupe, $H, N \lhd G$ des sous-groupes normaux tels que $N \subseteq H$. Alors, l'homomorphisme naturel de groupes*

$$\varphi : G/N \to G/H, \quad gN \mapsto gH$$

« induit » (par le théorème d'isomorphisme 2.4) l'isomorphisme de groupes

$$\overline{\varphi} : (G/N)/(H/N) \to G/H, \quad gN(H/N) \mapsto gH.$$

Démonstration. L'homomorphisme φ est visiblement surjectif et son noyau est composé des éléments $gN \in G/N$ tels que $gH = H$, donc $g \in H$, donc $gN \in H/N$, montrant $\ker(\varphi) = H/N$. L'existence de $\overline{\varphi}$ résulte donc d'une application directe du théorème d'isomorphisme 2.4. □

Plus de théorèmes d'isomorphisme pour les anneaux

Lemme 2.15. *Soient A un anneau commutatif et $I, J, K \trianglelefteq A$ des idéaux. Alors :*

(a) $I \cap J$ *est un idéal de* A.

(b) $I + J := \{i + j \mid i \in I, j \in J\}$ *est un idéal de* A.

(c) $I \cdot J := \{\sum_{\ell=1}^{r} i_\ell j_\ell \mid r \in \mathbb{N}, i_\ell \in I, j_\ell \in J\}$ *est un idéal de* A.

(d) $I + J = J + I$.

(e) $(I \cdot J) \cdot K = I \cdot (J \cdot K)$.

(f) $I \cdot (J + K) = I \cdot J + I \cdot K$.

Démonstration. Exercice sur la feuille 3. □

Lemme 2.16. *Soient A un anneau commutatif, $B \leq A$ un sous-anneau et $I, J \trianglelefteq A$ des idéaux. Alors :*

(a) $B \cap I$ *est un idéal de* B.

(b) $B + I := \{b + i \mid b \in B, i \in I\}$ *est un sous-anneau de* A.

(c) I *est un idéal de* $B + I$.

Démonstration. C'est clair ! □

Proposition 2.17 (Deuxième théorème d'isomorphisme)**.** *Soient A un anneau, $B \leq A$ un sous-anneau et $I \trianglelefteq A$ un idéal. Alors, l'homomorphisme naturel d'anneaux*

$$\varphi : B \to (B + I)/I, \quad b \mapsto b + I,$$

« induit » (par le théorème d'isomorphisme 2.9) l'isomorphisme d'anneaux

$$\overline{\varphi} : B/(B \cap I) \to (B + I)/I, \quad b + (B \cap I) \mapsto b + I.$$

Démonstration. Noter d'abord que le lemme 2.16 nous assure que tout est bien défini. L'homomorphisme φ est visiblement surjectif et son noyau est composé des éléments $b \in B$ tels que $b + I = I$, donc $b \in B \cap I$, montrant $\ker(\varphi) = B \cap I$. L'existence de $\overline{\varphi}$ résulte donc d'une application directe du théorème d'isomorphisme 2.9. □

Proposition 2.18 (Troisième théorème d'isomorphisme)**.** *Soient A un anneau et $I, J \trianglelefteq A$ des idéaux tels que $J \subseteq I$. Alors, l'homomorphisme naturel d'anneaux*

$$\varphi : A/J \to A/I, \quad a + J \mapsto a + I$$

« induit » (par le théorème d'isomorphisme 2.9) l'isomorphisme d'anneaux

$$\overline{\varphi} : (A/J)/(I/J) \to A/I, \quad a + J + (I/J) \mapsto a + I.$$

Démonstration. L'homomorphisme φ est visiblement surjectif et son noyau est composé des éléments $a+J \in A/J$ tels que $a+I = I$, donc $a \in I$, donc $a+J \in I/J$, montrant $\ker(\varphi) = I/J$. L'existence de $\overline{\varphi}$ résulte donc d'une application directe du théorème d'isomorphisme 2.9. □

Plus de théorèmes d'isomorphisme pour les espaces vectoriels

Proposition 2.19 (Deuxième théorème d'isomorphisme)**.** *Soient K un corps et V, W des K-espaces vectoriels. Alors, l'homomorphisme K-linéaire*

$$\varphi : V \to (V + W)/W, \quad v \mapsto v + W,$$

« induit » (par le théorème d'isomorphisme 2.11) l'isomorphisme K-linéaire

$$\overline{\varphi} : V/(V \cap W) \to (V + W)/W, \quad v + (V \cap W) \mapsto v + W.$$

Démonstration. Exercice sur la feuille 3. □

Proposition 2.20 (Troisième théorème d'isomorphisme)**.** *Soient K un corps et V un K-espace vectoriel et $W_1 \subseteq W_2$ deux sous-K-espaces de V. Alors, l'homomorphisme K-linéaire*

$$\varphi : V/W_1 \to V/W_2, \quad v + W_1 \mapsto v + W_2$$

« induit » (par le théorème d'isomorphisme 2.11) l'isomorphisme K-linéaire

$$\overline{\varphi} : (V/W_1)/(W_2/W_1) \to V/W_2, \quad v + W_1 + (W_2/W_1) \mapsto v + W_2.$$

Démonstration. Par le troisième théorème d'isomorphisme pour groupes 2.14 l'application $\overline{\varphi}$ est un isomorphisme de groupes. Donc il suffit de démontrer qu'elle est compatible avec la multiplication scalaire :

$$\begin{aligned}\overline{\varphi}(x.(v + W_1 + (W_2/W_1))) &= \overline{\varphi}(x.v + W_1 + (W_2/W_1)) = \\ &\varphi(x.v + W_1) = x.v + W_2 = x.(v + W_2) = x.\varphi(v + W_2) = x.\overline{\varphi}(v + W_1 + (W_2/W_1))\end{aligned}$$

pour tout $x \in K$ et tout $v \in V$. □

3 Compléments de la théorie des groupes

On commence par rappeler des définitions et propositions déjà démontrés au semestre précédent. Soit G un groupe. L'ordre ou le cardinal de G est son nombre d'éléments (si G est infini, alors on dit que son ordre est infini). Pour un élément $g \in G$ on définit *l'ordre* de g (notation : $\mathrm{ord}(g)$) comme le plus petit entier positif $n > 0$ tel que $g^n = 1$, l'élément neutre (si un tel n n'existe pas, alors on dit que $\mathrm{ord}(g) = \infty$). Rappelons la définition de g^n pour tout $n \in \mathbb{Z}$:

$$g^n = \begin{cases} 1 & \text{si } n = 0, \\ \underbrace{g \cdot g \cdot \ldots \cdot g}_{n\text{-fois}} & \text{si } n > 0, \\ \underbrace{g^{-1} \cdot g^{-1} \cdot \ldots \cdot g^{-1}}_{|n|\text{-fois}} & \text{si } n < 0. \end{cases}$$

Exemple 3.1. – *Dans tout groupe, l'ordre de l'élément neutre est* 1 *et c'est le seul élément d'ordre* 1.
– *Les ordres des éléments du groupe symétrique* S_3 *sont les suivants :*

$$\mathrm{ord}\big((1)\big) = 1, \ \ \mathrm{ord}\big((1\ 2)\big) = 2, \ \ \mathrm{ord}\big((1\ 3)\big) = 2,$$
$$\mathrm{ord}\big((2\ 3)\big) = 2, \ \ \mathrm{ord}\big((1\ 2\ 3)\big) = 3, \ \ \mathrm{ord}\big((1\ 3\ 2)\big) = 3.$$

– *Les ordres des éléments de* $(\mathbb{Z}/6\mathbb{Z}, +, \overline{0})$ *sont les suivants :*

$$\mathrm{ord}(\overline{0}) = 1, \ \ \mathrm{ord}(\overline{1}) = 6, \ \ \mathrm{ord}(\overline{2}) = 3, \ \ \mathrm{ord}(\overline{3}) = 2, \ \ \mathrm{ord}(\overline{4}) = 3, \ \ \mathrm{ord}(\overline{5}) = 6.$$

Donc $\mathbb{Z}/6\mathbb{Z}$ *est un groupe cyclique qui peut être engendré par* $\overline{1}$ *ou* $\overline{5} = \overline{-1}$.
– *Dans* $(\mathbb{Z}, +, 0)$*, l'ordre de tout* $0 \neq m \in \mathbb{Z}$ *est infini (car* $nm \neq 0$ *pour tout* $n \in \mathbb{N}_{>0}$*).*

Soit G encore un groupe et $g \in G$ un élément d'ordre fini $n := \mathrm{ord}(g)$. Alors, le noyau de l'homomorphisme de groupes

$$\varphi : \mathbb{Z} \to G, \quad m \mapsto g^m$$

est égal à $n\mathbb{Z}$. Donc par le premier théorème d'isomorphisme 2.4 on obtient l'isomorphisme de groupes

$$\overline{\varphi} : \mathbb{Z}/n\mathbb{Z} \to \mathrm{im}(\varphi) \subseteq G, \quad \overline{m} \mapsto g^m.$$

Rappelons aussi la notation $\langle g_1, \ldots, g_r \rangle$ pour le sous-groupe de G engendré par $g_1, \ldots, g_r \in G$. Ce sous-groupe est l'ensemble de tous les éléments de G qui s'écrivent comme produit fini de

$$g_1, \ldots, g_r, g_1^{-1}, \ldots, g_r^{-1}$$

où on peut utiliser les éléments plusieurs (ou aucune) fois et dans un ordre quelconque. En particulier, $\langle g \rangle$ est l'ensemble $\{g^m \mid m \in \mathbb{Z}\}$. Donc si $\mathrm{ord}(g) = n < \infty$, alors

$$\overline{\varphi} : \mathbb{Z}/n\mathbb{Z} \to \langle g \rangle, \quad \overline{m} \mapsto g^m$$

est un isomorphisme de groupes. Cela montre qu'à isomorphisme près tout groupe cyclique d'ordre n est de la forme $\mathbb{Z}/n\mathbb{Z}$. En plus, nous trouvons

$$\mathrm{ord}(g) = \#\langle g \rangle,$$

en mots : l'ordre du sous-groupe engendré par g est égal à l'ordre de g.

Théorème 3.2 (Lagrange, théorème 8.6 d'Algèbre 1)**.** *Soient G un groupe et $H \leq G$ un sous-groupe. Alors :*

$$\#G = (G : H) \cdot \#H.$$

On déduit du théorème de Lagrange la divisibilité

$$\mathrm{ord}(g) \mid \#G$$

pour tout groupe fini G et tout $g \in G$. En conséquence, nous trouvons aussi le « petit Fermat de la théorie des groupes »

$$g^{\#G} = 1.$$

Nous voulons maintenant classifier tous les groupes de cardinal ≤ 7. Pour ceci nous avons encore besoin d'énoncer un lemme du semestre précédent.

Lemme 3.3 (Lemme 9.9 d'Algèbre 1)**.** *Soient G un groupe abélien fini et $H_1, H_2 \leq H$ deux sous-groupes de G.*

(a) Si $H_1 \cap H_2 = \{1\}$, alors, l'application $\phi : H_1 \times H_2 \to G$ donné par $(h_1, h_2) \mapsto h_1 h_2$ est un homomorphisme de groupes injectif.

(b) Si $\mathrm{pgcd}(\#H_1, \#H_2) = 1$, alors $H_1 \cap H_2 = \{1\}$.

Exemple 3.4. *Nous faisons la liste de tous les groupes d'ordre ≤ 7 à isomorphisme près.*

– *Le seul groupe d'ordre 1 est le groupe trivial ; son seul élément est l'élément neutre.*

– *$n = 2, 3, 5, 7$. Comme tout groupe d'ordre premier est cyclique, il en suit que le seul groupe d'ordre n à isomorphisme près est $\mathbb{Z}/n\mathbb{Z}$.*

– *$n = 4$: Nous connaissons deux groupes d'ordre 4 : $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ qui ne sont pas isomorphes (le premier est cyclique et le deuxième non-cyclique). On va démontrer qu'il n'y en a pas plus ; on en déduira notamment que tout groupe d'ordre 4 est abélien.*
  Soit G un groupe d'ordre 4 qui n'est pas cyclique (s'il est cyclique, il est isomorphe à $\mathbb{Z}/4\mathbb{Z}$). On choisit $a \neq b$ deux éléments de G qui ne sont pas l'élément neutre. On a $\mathrm{ord}(a) \mid \#G$, donc $\mathrm{ord}(a) = 2$, car s'il était 4, le groupe serait cyclique engendré par a. Le même argument montre $\mathrm{ord}(b) = 2$. On a $\langle a \rangle \cap \langle b \rangle = \{1\}$. Soit $c := ab$. Il est clair que $c \neq 1, a, b$. Par le même argument $ba \neq 1, a, b$, donc $c = ba$. Donc G est abélien. Par le lemme 3.3 (a) nous obtenons que $\langle a \rangle \times \langle b \rangle$ est isomorphe à G. Donc $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

– *$n = 6$. Nous connaissons deux groupes d'ordre 6 : $\mathbb{Z}/6\mathbb{Z}$ et S_3 qui ne sont pas isomorphes (par exemple : le premier est abélien et le deuxième non-abélien). On va démontrer qu'il n'y en a pas plus.*
  Soit G un groupe d'ordre 6 qui n'est pas cyclique (s'il est cyclique, il est isomorphe à $\mathbb{Z}/6\mathbb{Z}$).
  Soit $g \in G$ différent de l'élément neutre. Comme l'ordre de g est un diviseur de 6 et strictement plus petit que 6 (sinon le groupe serait cyclique engendré par g), on a $\mathrm{ord}(g) = 2$ ou $\mathrm{ord}(g) = 3$. On veut démontrer qu'il existe $a, b \in G$ tels que $\mathrm{ord}(a) = 3$ et $\mathrm{ord}(b) = 2$.
  Si tout élément non-neutre de G était d'ordre 2, G serait abélien par l'exercice 5 de la feuille 5 d'Algèbre 1. En choisissant $b_1 \neq b_2$ d'ordre 2, le lemme 3.3 (a) nous donne une injection $\phi : \langle b_1 \rangle \times \langle b_2 \rangle \to G$. L'image de ϕ serait un sous-groupe d'ordre 4, mais $4 \nmid 6$, c'est une contradiction avec le théorème de Lagrange 3.2.

Soit donc a un élément d'ordre 3. On choisit $b \notin \langle a \rangle =: H$. Comme $G = H \sqcup bH$, il en suit que $b^2 \in H$ ou $b^2 \in bH$. La deuxième possibilité est impossible (sinon b serait dans H). Donc $b^2 \in H$. Donc $\mathrm{ord}(b^2)$ est 1 ou 3. Le dernier cas mènerait à $\mathrm{ord}(b) = 6$ qui est exclu. Donc $\mathrm{ord}(b) = 2$.
Notons que $ab \neq 1, a, a^2, b$. On a aussi $a^2b \neq 1, a, a^2, b, ab$. Donc $G = \{1, a, a^2, b, ab, a^2b\}$. Si $ba = ab$, alors G serait abélien et dans ce cas $\mathrm{ord}(ab) = 6$ et le groupe serait cyclique ce que nous supposons ne pas être le cas. La seule autre possiblité est $ba = a^2b$.
Dans S_3 nous posons $A := (1\ \ 2\ \ 3)$ et $B := (1\ \ 2)$. Nous définissons $\phi : S_3 \to G$ par $\phi(\mathrm{id}) = 1$, $\phi(A) = a$, $\phi(A^2) = a^2$, $\phi(B) = b$, $\phi(AB) = ab$, et $\phi(A^2B) = a^2b$. C'est clairement une bijection. Que c'est un homomorphisme est une conséquence de $\mathrm{ord}(A) = 3$, $\mathrm{ord}(B) = 2$ et $BA = A^2B$ qui est facilement vérifié.

Sans démonstration on énonce la classification des groupes abéliens de type fini. Si nous avons du temps à la fin du cours, on démontrera ce théorème.

Théorème 3.5 (Classification des groupes abéliens de type fini)**.** *Soit G un groupe abélien de type fini (c'est-à-dire que G peut être engendré par un nombre fini d'éléments). Alors, il existe des uniques $r, s \in \mathbb{N}$ et des uniques $d_1, d_2, \ldots, d_s \in \mathbb{N}_{\geq 2}$ tels que*
– *$d_1 \mid d_2 \mid \cdots \mid d_s$ et*
– *$G \cong \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_s\mathbb{Z}$.*

Exemple 3.6. *On obtient du théorème 3.5 qu'à isomorphisme près il n'existe que deux groupes abéliens de cardinal 12, en l'occurence $\mathbb{Z}/12\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.*

4 Polynômes

Convention : à partir de maintenant tout anneau est supposé commutatif, sauf si le contraire est explicitement mentionné.
Nous avons déjà utilisé des polynômes car ils sont connus de l'école et du cours d'analyse. Maintenant nous allons en donner un traitement plus rigoureux.

Définition 4.1. *Soit A un anneau (commutatif !).*
– *Un* polynôme à coefficients dans *A (pour la variable X) est une « somme formelle » $\sum_{i=0}^{n} a_i X^i$ où $n \in \mathbb{N}$ et $a_0, \ldots, a_n \in A$.*
Ici, X n'est qu'un symbole. Nous pouvons le remplacer par tout autre symbole, par exemple Y, x, t, T, etc.
– *(Définition plus formelle :) Un* polynôme à coefficients dans *A est une application $a : \mathbb{N} \to A$ telle qu'il existe $n \in \mathbb{N}$ tel que pour tout $m > n$ on a $a(m) = 0$.*
Si a est une telle application, nous écrivons $\sum_{i=0}^{n} a(i) X^i$.
– *Nous notons $A[X]$ l'ensemble de tous les polynômes à coefficients dans A pour la variable X.*
– *Soit $f(X) = \sum_{i=0}^{n} a_i X^i \in A[X]$. Le* degré *de f (notation : $\deg(f)$) est l'entier m maximal tel que $a_m \neq 0$. Si $f = 0$, alors on pose $\deg(f) = -\infty$. On appelle $a_d X^d$ avec $d = \deg(f)$ le* monôme dominant *de f. On appelle f* unitaire *si $a_{\deg(f)} = 1$.

– *Soient* $f(X) = \sum_{i=0}^{n} a_i X^i$ *et* $g(X) = \sum_{j=0}^{m} b_i X^i$ *deux éléments de* $A[X]$. *Nous définissons la* somme *de ces deux polynômes comme :*

$$f(X) + g(X) = \sum_{i=0}^{\max(n,m)} (a_i + b_i) X^i,$$

où on suppose $a_i = 0$ *si* $i > n$ *et* $b_j = 0$ *si* $j > m$.

– *Soient* $f(X) = \sum_{i=0}^{n} a_i X^i$ *et* $g(X) = \sum_{j=0}^{m} b_i X^i$ *deux éléments de* $A[X]$. *Nous définissons le* produit *de ces deux polynômes comme :*

$$f(X) \cdot g(X) = \sum_{k=0}^{n+m} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) X^k,$$

où on suppose $a_i = 0$ *si* $i > n$ *et* $b_j = 0$ *si* $j > m$.

Remarque 4.2. *Il faut bien faire la différence entre un polynôme et la fonction qu'il représente : par exemple pour* $A = \mathbb{F}_2$, *les polynômes* $f(X) = X$ *et* $g(X) = X^3$ *sont différents, mais,* $f(b) = b = g(b)$ *pour tout* $b \in \mathbb{F}_2$, *donc vus comme des fonctions* $\mathbb{F}_2 \to \mathbb{F}_2$ *ils sont égaux !*

Proposition 4.3. *Soit* A *un anneau (commutatif !). Alors,* $(A[X], +, \cdot, 0, 1)$ *est un anneau commutatif.*

Démonstration. La vérification est facile. On ne la fera pas. □

Lemme 4.4. *Soient* A *un anneau et* $f, g \in A[X]$.

(a) $\deg(f+g) \leq \max(\deg(f), \deg(g))$ et $\deg(fg) \leq \deg(f) + \deg(g)$.

(b) Soient $f(X) = \sum_{i=0}^{n} a_i X^i$ *et* $g(X) = \sum_{j=0}^{m} b_i X^i$ *où on suppose* $n = \deg(f)$ *et* $m = \deg(g)$. *Si* $a_n \in A^\times$ *ou* $b_m \in A^\times$, *alors* $\deg(fg) = \deg(f) + \deg(g)$.

Démonstration. (a) C'est évident de la définition de la somme et du produit de deux polynômes. Mais, notez que si $f = 0$ nous devons faire le calcul $-\infty + \deg(g) = -\infty$; donc, nous calculons avec le symbole ∞ d'une façon naïve (sans en donner un traitement formel).
(b) Par hypothèse on a $a_n b_m \neq 0$. Donc, $a_n b_m X^{n+m}$ est le monôme dominant de $f \cdot g$. □

On rappelle la définition d'anneau intègre.

Définition 4.5 (Algèbre 1, Définition 5.11)**.** *Soit* A *un anneau.*
Un élément $a \in A$ *est appelé* diviseur de zéro *s'il existe* $b \in A \setminus \{0\}$ *tel que* $a \cdot b = 0$.
Un anneau A *est appelé* intègre *si* 0 *est le seul diviseur de zéro (*$\Leftrightarrow$ *pour tout* $0 \neq a, b \in A$ *on a* $a \cdot b \neq 0$*).*

Exemple 4.6. – *Tout corps est un anneau intègre : Si* $0 = ab$ *avec* $a \neq 0$, *alors* $0 = a^{-1}0 = a^{-1}ab = b$.

– $\mathbb{Z}/n\mathbb{Z}$ *pour* $n \in \mathbb{N}_{\geq 2}$ *est un anneau intègre si et seulement si* n *est un nombre premier.*
Raison : Si n *n'est pas un nombre premier, alors* $n = ab$ *avec* $a > 1$ *et* $b > 1$ *; donc* $\overline{a}\overline{b} = \overline{n} = \overline{0}$, *mais* $\overline{a} \neq 0 \neq \overline{b}$. *Si* $\mathbb{Z}/n\mathbb{Z}$ *n'est pas un anneau intègre, alors, il existe* $1 \leq a, b \leq n-1$ *tels que* $\overline{a}\overline{b} = \overline{0}$, *donc* $n \mid ab$, *mais* $n \nmid a$ *et* $n \nmid b$, *montrant que* n *n'est pas un nombre premier (par le lemme 5.33 d'Algèbre 1).*
En plus, on rappelle que $\mathbb{Z}/n\mathbb{Z}$ *est un corps si et seulement si* n *est un nombre premier (comme nous l'avons vu : Algèbre 1, Cor. 5.32).*

Proposition 4.7. *Soient A un anneau intègre et $f, g \in A[X]$. Alors* $\deg(fg) = \deg(f) + \deg(g)$.

Démonstration. C'est une conséquence directe de la démonstration du lemme 4.4(b). □

Corollaire 4.8. *Soit A un anneau intègre. Alors, $(A[X])^\times = A^\times$, c'est-à-dire que les seules unités de $A[X]$ sont les polynômes constants où la constante est une unité de A.*

Démonstration. Il est clair que les polynômes constants où la constante est une unité de A appartiennent à $(A[X])^\times$. Soit $f(X) = \sum_{i=0}^{n} a_i X^i$ un polynôme de degré n dans $(A[X])^\times$. Alors par définition il existe $g(X) = \sum_{j=0}^{m} b_i X^i$ (on suppose $m = \deg(g)$) tel que $f(X)g(X) = 1$ (polynôme constant). Par la proposition 4.7 nous obtenons $n+m = 0$. Comme $n, m \geq 0$ (il est clair que f et g ne sont pas égaux au polynôme constant 0), on en conclut $n = m = 0$, alors $f(X) = a_0$ et $g(X) = b_0$. L'égalité $1 = a_0 b_0$ montre $f = a_0 \in A^\times$. □

Théorème 4.9 (Division euclidienne)**.** *Soient A un anneau et $g = \sum_{i=0}^{d} b_i X^i \in A[X]$ un polynôme de degré $d \geq 0$. On suppose $b_d \in A^\times$ (cette hypothèse n'est pas nécessaire si A est un corps).*
Alors, pour tout polynôme $f \in A[X]$ il existe des uniques polynômes $q, r \in A[X]$ tels que

$$f = qg + r \quad \text{et} \quad \deg(r) < d.$$

Démonstration. Soit $f(X) = \sum_{i=0}^{n} a_i X^i \in A[X]$ de degré n.
Existence : Nous montrons l'existence par récurrence sur n. Si $n < d$, on pose $q = 0$ et $r = f$ et on a terminé. Supposons donc $n \geq d$ et que l'existence est déjà connue pour tous les polynômes de degré strictement plus petit que n. On pose

$$f_1(X) := f(X) - a_n \cdot b_d^{-1} X^{n-d} g(X).$$

C'est un polynôme de degré au plus $n-1$ parce que nous avons annulé le coefficient devant X^n. Alors, par hypothèse de récurrence il existe $q_1, r_1 \in A[X]$ tels que $f_1 = q_1 g + r_1$ et $\deg(r_1) < d$. Donc

$$f(X) = f_1(X) + a_n b_d^{-1} g(X) X^{n-d} = q(X)g(X) + r_1(X)$$

où $q(X) := q_1(X) + a_n b_d^{-1} X^{n-d}$ et nous avons démontré l'existence.
Unicité : Supposons $f = qg + r = q_1 g + r_1$ avec $q, q_1, r, r_1 \in A[X]$ et $\deg(r), \deg(r_1) < d$. Alors $g(q - q_1) = r_1 - r$. Si $q = q_1$, alors $r = r_1$ et on a terminé. Si $q \neq q_1$, alors $\deg(q - q_1) \geq 0$ et par le lemme 4.4(b) on trouve $\deg(g(q - q_1)) \geq \deg(g) = d = \deg(r_1 - r)$. La dernière égalité contredit lemme 4.4, donc $q \neq q_1$ ne peut pas apparaître. □

Exemple 4.10. *Exemple d'un calcul d'une division euclidienne au tableau...*

Nous allons voir dans la section prochaine que la division euclidienne nous permet de généraliser l'algorithme d'Euclide pour le calcul d'un pgcd. Ici on continue d'abord par une propriété très importante de l'anneau des polynômes qui s'appelle aussi « propriété universelle ».

Proposition 4.11. *Soient A, B des anneaux, $\varphi : A \to B$ un homomorphisme d'anneaux et $b \in B$. Alors il existe un unique homomorphisme d'anneaux*

$$\Phi : A[X] \to B$$

qui a les propriétés

– $\Phi(X) = b$ *et*
– $\Phi(a) = \varphi(a)$ *pour tout* $a \in A$.
Dans ce cas nous avons pour $f = \sum_{i=0}^{n} a_i X^i$

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

En particulier, $\mathrm{im}(\Phi) = \Phi(A[X]) \subseteq B$ *est un sous-anneau.*

Démonstration. **Unicité :** Si un tel Φ existe, il doit satisfaire

$$\Phi(\sum_{i=0}^{n} a_i X^i) = \sum_{i=0}^{n} \Phi(a_i)\Phi(X)^i = \sum_{i=0}^{n} \varphi(a_i) b^i$$

par les propriétés des homomorphismes d'anneaux. Donc, si un tel Φ existe, il est nécessairement unique.
Existence : On définit

$$\Phi(\sum_{i=0}^{n} a_i X^i) := \sum_{i=0}^{n} \varphi(a_i) b^i$$

pour tout polynôme $\sum_{i=0}^{n} a_i X^i \in A[X]$. Nous devons montrer qu'avec cette définition Φ est un homomorphisme d'anneaux :
– $\Phi(1) = \varphi(1) = 1$.
– $\Phi(f+g) = \Phi(\sum_{i=0}^{n} a_i X^i + \sum_{j=0}^{m} c_j X^j) = \Phi(\sum_{i=0}^{\max(n,m)} (a_i + c_i) X^i) = \sum_{i=0}^{\max(n,m)} \varphi(a_i + c_i) b^i$
$= \sum_{i=0}^{n} \varphi(a_i) b^i + \sum_{j=0}^{m} \varphi(c_j) b^j = \Phi(\sum_{i=0}^{n} a_i X^i) + \Phi(\sum_{j=0}^{m} c_j X^j) = \Phi(f) + \Phi(g)$.
– $\Phi(f \cdot g) = \Phi((\sum_{i=0}^{n} a_i X^i) \cdot (\sum_{j=0}^{m} c_j X^j)) = \Phi(\sum_{k=0}^{n+m} (\sum_{i=0}^{k} a_i c_{k-i}) X^k)$
$= \sum_{k=0}^{n+m} \varphi(\sum_{i=0}^{k} a_i c_{k-i}) b^k = (\sum_{i=0}^{n} \varphi(a_i) b^i) \cdot (\sum_{j=0}^{m} \varphi(c_j) b^j)$
$= \Phi(\sum_{i=0}^{n} a_i X^i) \cdot \Phi(\sum_{j=0}^{m} c_j X^j) = \Phi(f) \cdot \Phi(g)$.
La dernière assertion provient juste du fait général que l'image de tout homomorphisme d'anneaux est un sous-anneau. □

Exemple 4.12. *Soit* $i = \sqrt{-1} \in \mathbb{C}$. *Soit* $\varphi : \mathbb{Q} \to \mathbb{C}$ *l'identité* $a \mapsto a$ *(on voit tout nombre rationnel comme un nombre complexe). La proposition 4.11 nous donne*

$$\Phi : \mathbb{Q}[X] \to \mathbb{C}, \quad \Phi(f) = \sum_{k=0}^{n} a_k i^k = \sum_{k=0,\ \text{pair}}^{n} (-1)^{k/2} a_k + i\Big(\sum_{k=0,\ \text{impair}}^{n} (-1)^{(k-1)/2} a_k\Big).$$

Alors, $\mathrm{im}(\Phi) = \{a + ib \mid a, b \in \mathbb{Q}\}$ *est un sous-anneau de* $\mathbb{C}$*, qu'on note* $\mathbb{Q}[i]$*. C'est même un sous-corps de* $\mathbb{C}$*, car tout élément non nul possède un inverse :*

$$(a + ib) \cdot \big(\frac{a}{a^2 + b^2} - i\frac{b}{a^2 + b^2}\big) = 1.$$

On peut remplacer $\mathbb{Q}$ *par* $\mathbb{Z}$ *pour obtenir l'anneau intègre* $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ *(qui n'est pas un corps, mais un anneau euclidien – voir la prochaine section).*

5 Anneaux euclidiens

Nous connaissons deux anneaux dans lesquels il existe une division euclidienne : les entiers relatifs et l'anneau des polynômes à coefficients dans un corps. Donc, ces deux anneaux – qui de loin semblent être très différents – ont cette propriété importante en commun.
Dans cette section nous allons faire une étape importante d'abstraction : nous formalisons l'idée de la division euclidienne et nous prenons l'idée abstraite comme base pour la définition d'une nouvelle classe d'anneaux : les anneaux euclidiens.
Nous allons aussi voir que dans les anneaux euclidiens, (l'analogue de) l'algorithme d'Euclide nous permet de calculer des plus grands diviseurs communs, des plus petits multiples communs, et des identités de Bézout.

Nous comparons maintenant la division euclidienne dans $\mathbb{Z}$ et $K[X]$ où K est un corps.

$\mathbb{Z}$	$K[X]$
Pour tout $a, b \in \mathbb{Z}$, $b \neq 0$	Pour tout $a, b \in K[X]$, $b \neq 0$
$\exists\, q, r \in \mathbb{Z}$ t.q.	$\exists\, q, r \in K[X]$ t.q.
$a = bq + r$ et	$a = bq + r$ et
$\lvert r\rvert < \lvert b\rvert$	$\deg(r) < \deg(b)$

Nous avons pris la définition $\deg(0) = -\infty$ pour que la formule $\deg(fg) = \deg(f) + \deg(g)$ soit toujours correcte (si les coefficients sont dans un anneau intègre ou un corps). On pourrait trouver cette convention gênante ; on peut s'en passer par l'équivalence :

$$\deg(r) < \deg(b) \Leftrightarrow (r = 0 \text{ ou } \deg(r) < \deg(b))\,.$$

On peut donc remplacer la dernière règle pour obtenir :

$\mathbb{Z}$	$K[X]$
Pour tout $a, b \in \mathbb{Z}$, $b \neq 0$	Pour tout $a, b \in K[X]$, $b \neq 0$
$\exists\, q, r \in \mathbb{Z}$ t.q.	$\exists\, q, r \in K[X]$ t.q.
$a = bq + r$ et	$a = bq + r$ et
($r = 0$ ou $\lvert r\rvert < \lvert b\rvert$)	($r = 0$ ou $\deg(r) < \deg(b)$)

Nous voyons que toutes les règles sont les mêmes sauf une partie de la dernière. Qu'est-ce que la valeur absolue d'un entier et le degré d'un polynôme ont en commun ? Ce sont tous les deux des « mesures de taille » ! On peut et doit être plus précis :

$\mathbb{Z}$	$K[X]$
Pour tout $0 \neq r \in \mathbb{Z}$	Pour tout $0 \neq r \in K[X]$
$\lvert r\rvert$ est un nombre naturel	$\deg(r)$ est un nombre naturel

Donc, $|\cdot|$ (pour $A := \mathbb{Z}$) et $\deg$ (pour $A := K[X]$) sont des applications de la forme $\delta : A \setminus \{0\} \to \mathbb{N}_{\geq 0}$. Nous ajoutons la formalisation dans une troisième colonne.

$\mathbb{Z}$	$K[X]$	A
Pour tout $a, b \in \mathbb{Z}$, $b \neq 0$	Pour tout $a, b \in K[X]$, $b \neq 0$	Pour tout $a, b \in A$, $b \neq 0$
$\exists\, q, r \in \mathbb{Z}$ t.q.	$\exists\, q, r \in K[X]$ t.q.	$\exists\, q, r \in A$ t.q.
$a = bq + r$ et	$a = bq + r$ et	$a = bq + r$ et
($r = 0$ ou $\lvert r\rvert < \lvert b\rvert$)	($r = 0$ ou $\deg(r) < \deg(b)$)	($r = 0$ ou $\delta(r) < \delta(b)$)

La formalisation dans la troisième colonne devient notre définition d'un anneau euclidien :

Définition 5.1. *Soit A un anneau intègre. A est appelé* anneau euclidien *s'il existe une application*

$$\delta : A \setminus \{0\} \to \mathbb{N}_{\geq 0}$$

telle que pour tout $a, b \in A$ avec $b \neq 0$ il existe $q, r \in A$ qui satisfont

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

Exemple 5.2. – *$\mathbb{Z}$ est un anneau euclidien avec $\delta(n) := |n|$ pour $n \in \mathbb{Z} \setminus \{0\}$.*
– *$K[X]$ (pour K un corps) est un anneau euclidien avec $\delta(f) := \deg(f)$ pour $f \in K[X] \setminus \{0\}$.*
– *$\mathbb{Z}[i] := \{a + ib \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ est un anneau euclidien avec $\delta(a + ib) := a^2 + b^2$ pour $a + ib \in \mathbb{Z}[i] \setminus \{0\}$ (exercice).*

Rappelons la définition du plus grand diviseur commun dans $\mathbb{Z}$ (Algèbre 1, déf. 5.23) :

Définition 5.3. *Soient $d \in \mathbb{Z}$ et $x, y \in \mathbb{Z}$. On appelle d un* plus grand diviseur commun de x, y *(notation : $d = \operatorname{pgcd}(x, y)$) si*
– *$d \mid x$ et $d \mid y$ et*
– *pour tout $e \in \mathbb{Z}$ on a $((e \mid x \text{ et } e \mid y) \Rightarrow e \mid d)$.*

En fait, on a fait un très petit changement : en Algèbre 1 nous avons imposé que d (et e) soit dans $\mathbb{N}$. Comme on veut faire une généralisation aux anneaux généraux, on ne peut pas utiliser $\mathbb{N}$. Avec la définition ci-dessus, 4 et -4 sont tous les deux des plus grands diviseurs communs de 8 et 12. En fait, si d est un plus grand commun diviseur de deux entiers, alors $-d$ l'est aussi. Donc le plus grand diviseur commun de deux entiers n'est pas unique : si l'on a un, on obtient l'autre en multipliant le premier par l'unité -1.
Nous généralisons maintenant la définition du plus grand diviseur commun en suivant mot à mot la définition 5.3.

Définition 5.4. *Soit A un anneau et soient $d, x, y \in A$. On appelle d un* plus grand diviseur commun de x, y *(notation : $\operatorname{pgcd}(x, y)$) si*
– *$d \mid x$ et $d \mid y$ et*
– *pour tout $e \in A$ on a $((e \mid x \text{ et } e \mid y) \Rightarrow e \mid d)$.*

On définit également le plus petit multiple commun dans un anneau général en reprenant la définition dans $\mathbb{Z}$ (Algèbre 1, déf. 5.27, encore, en remplaçant $\mathbb{N}$ par $\mathbb{Z}$).

Définition 5.5. *Soient $m \in A$ et $x, y \in A$. On appelle m un* plus petit multiple commun de x, y *(notation : $\operatorname{ppcm}(x, y)$) si*

– $x \mid m$ *et* $y \mid m$ *et*
– *pour tout* $n \in A$ *on a* $((x \mid n$ *et* $y \mid n) \Rightarrow m \mid n)$.

Attention ! Dans un anneau quelconque, ni pgcd ni ppcm n'existent en général ! Par contre pour $\mathbb{Z}$ nous avons démontré – à l'aide de l'algorithme d'Euclide, donc du fait que $\mathbb{Z}$ est un anneau euclidien – (Algèbre 1, prop. 5.24) que un/le pgcd (et aussi un/le ppcm) existe toujours et qu'il y a toujours une identité de Bézout. La même chose est vraie pour tous les anneaux euclidiens, comme on va le voir tout de suite.
D'abord encore une nouvelle définition pour bien exprimer la relation entre deux pgcd des mêmes nombres.

Définition 5.6. *Soit A un anneau intègre. On appelle $a, b \in A$* associés *s'il existe $u \in A^\times$ (une unité) tel que $a = ub$. Notation : $a \sim b$.*

Exemple 5.7. *Comme les seules unités de $\mathbb{Z}$ sont 1 et -1, le seul élément de $\mathbb{Z}$ qui est associé à un élément $n \in \mathbb{Z}$ est $-n$.*

Lemme 5.8. *Être associés définit une relation d'équivalence sur l'anneau A.*

Démonstration. **Réflexivité** Soit $a \in A$. Alors $a \sim a$ car $a = 1 \cdot a$.

Symétrie Soient $a, b \in A$ tels que $a \sim b$. Il existe $u \in A^\times$ tel que $a = ub$. Donc $b = u^{-1}a$, donc $b \sim a$.

Transitivité Soient $a, b, c \in A$ tels que $a \sim b$ et $b \sim c$. Il existe $u, v \in A^\times$ tels que $a = ub$ et $b = vc$. Donc $a = uvc$ et $a \sim c$ car $uv \in A^\times$.

□

Proposition 5.9. *Soient A un anneau intègre et $a, b \in A$ deux éléments.*

(a) Si $a \mid b$ et $b \mid a$, alors $a \sim b$.

(b) Tous les pgcd de a et b sont associés. Plus précisement, si $d, e \in A$ sont tous les deux un plus grand diviseur commun de a et b, alors $d \sim e$. Nous écrivons $\mathrm{pgcd}(a, b) \sim d$.

(c) Tous les ppcm de a et b sont associés. Plus précisement, si $m, n \in A$ sont tous les deux un plus petit multiple commun de a et b, alors $m \sim n$. Nous écrivons $\mathrm{ppcm}(a, b) \sim n$.

Démonstration. (a) Il existe $r, s \in A$ tels que $a = rb$ et $b = sa$. Donc $a = rsa$ et $0 = a(1 - rs)$. En utilisant le fait que A est intègre, on conclut $1 - rs = 0$, donc $rs = 1$, donc $r, s \in A^\times$, donc $a \sim b$.
(b) et (c) sont une conséquence directe de (a) et de la deuxième partie de la définition du pgcd/ppcm.
□

Théorème 5.10 (Algorithme d'Euclide, identité de Bézout)**.** *Soit A un anneau euclidien (avec δ comme dans la définition 5.1). Alors, pour tout $a, b \in A$, un plus grand commun diviseur $d \sim \mathrm{pgcd}(a, b)$ existe et il existe $r, s \in A$ tels que*

$$d = ra + sb.$$

Démonstration. On montre que l'algorithme d'Euclide donne le résultat.

– Préparation : On pose
$$\begin{cases} x_0 = a,\ x_1 = b & \text{si } \delta(a) \geq \delta(b), \\ x_0 = b,\ x_1 = a & \text{sinon.} \end{cases}$$
On pose aussi $B_0 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.
– Si $x_1 = 0$, on **arrête** et on pose $d := x_0$.
Si $x_1 \neq 0$, on fait la division euclidienne
$$x_0 = x_1 q_1 + x_2 \quad \text{où } q_1, x_2 \in A \text{ tels que } (x_2 = 0 \text{ ou } \delta(x_2) < \delta(x_1)).$$
On pose $A_1 := \left(\begin{smallmatrix} -q_1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $B_1 := A_1 B_0$.
On a $\left(\begin{smallmatrix} x_2 \\ x_1 \end{smallmatrix}\right) = A_1 \left(\begin{smallmatrix} x_1 \\ x_0 \end{smallmatrix}\right) = B_1 \left(\begin{smallmatrix} x_1 \\ x_0 \end{smallmatrix}\right)$.
– Si $x_2 = 0$, on **arrête** et on pose $d := x_1$.
Si $x_2 \neq 0$, on fait la division euclidienne
$$x_1 = x_2 q_2 + x_3 \quad \text{où } q_2, x_3 \in A \text{ tels que } (x_3 = 0 \text{ ou } \delta(x_3) < \delta(x_2)).$$
On pose $A_2 := \left(\begin{smallmatrix} -q_2 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $B_2 := A_2 B_1$.
On a $\left(\begin{smallmatrix} x_3 \\ x_2 \end{smallmatrix}\right) = A_2 \left(\begin{smallmatrix} x_2 \\ x_1 \end{smallmatrix}\right) = B_2 \left(\begin{smallmatrix} x_1 \\ x_0 \end{smallmatrix}\right)$.
– Si $x_3 = 0$, on **arrête** et on pose $d := x_2$.
Si $x_3 \neq 0$, on fait la division euclidienne
$$x_2 = x_3 q_3 + x_4 \quad \text{où } q_3, x_4 \in A \text{ tels que } (x_4 = 0 \text{ ou } \delta(x_4) < \delta(x_3)).$$
On pose $A_3 := \left(\begin{smallmatrix} -q_3 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $B_3 := A_3 B_2$.
On a $\left(\begin{smallmatrix} x_4 \\ x_3 \end{smallmatrix}\right) = A_3 \left(\begin{smallmatrix} x_3 \\ x_2 \end{smallmatrix}\right) = B_3 \left(\begin{smallmatrix} x_1 \\ x_0 \end{smallmatrix}\right)$.
– $\cdots$
– Si $x_n = 0$, on **arrête** et on pose $d := x_{n-1}$.
Si $x_n \neq 0$, on fait la division euclidienne
$$x_{n-1} = x_n q_n + x_{n+1} \quad \text{où } q_n, x_{n+1} \in A \text{ tels que } (x_{n+1} = 0 \text{ ou } \delta(x_{n+1}) < \delta(x_n)).$$
On pose $A_n := \left(\begin{smallmatrix} -q_n & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $B_n := A_n B_{n-1}$.
On a $\left(\begin{smallmatrix} x_{n+1} \\ x_n \end{smallmatrix}\right) = A_n \left(\begin{smallmatrix} x_n \\ x_{n-1} \end{smallmatrix}\right) = B_n \left(\begin{smallmatrix} x_1 \\ x_0 \end{smallmatrix}\right)$.
– $\cdots$

Il est clair que l'algorithme ci-dessus (c'est l'algorithme d'Euclide !) s'arrête car
$$\delta(x_n) < \delta(x_{n-1}) < \cdots < \delta(x_2) < \delta(x_1)$$
sont des nombres naturels.
Supposons que l'algorithme termine avec $x_n = 0$. Donc, $d = x_{n-1}$. Nous avons par construction :
$$\left(\begin{smallmatrix} x_n \\ x_{n-1} \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 \\ d \end{smallmatrix}\right) = B_{n-1} \left(\begin{smallmatrix} x_1 \\ x_0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} \alpha & \beta \\ r & s \end{smallmatrix}\right) \left(\begin{smallmatrix} x_1 \\ x_0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} \alpha x_1 + \beta x_0 \\ r x_1 + s x_0 \end{smallmatrix}\right),$$
montrant
$$d = r x_1 + s x_0.$$

Noter que le déterminant de A_i est -1 pour tout i, donc $\det(B_{n-1}) = (-1)^{n-1}$. Alors $C := (-1)^{n-1}\left(\begin{smallmatrix} s & -\beta \\ -r & \alpha \end{smallmatrix}\right)$ est l'inverse de B_{n-1}. Donc

$$\left(\begin{smallmatrix} x_1 \\ x_0 \end{smallmatrix}\right) = CB_{n-1}\left(\begin{smallmatrix} x_1 \\ x_0 \end{smallmatrix}\right) = C\left(\begin{smallmatrix} 0 \\ d \end{smallmatrix}\right) = \left(\begin{smallmatrix} d(-1)^n\beta \\ d(-1)^{n-1}\alpha \end{smallmatrix}\right),$$

montrant $d \mid x_1$ et $d \mid x_0$. Ceci montre que d est un pgcd de x_0 et x_1. □

Corollaire 5.11. *Soient A un anneau euclidien et $a, b, d, y \in A$.*

(a) Si $d \sim \operatorname{pgcd}(a, b)$, alors $1 \sim \operatorname{pgcd}(\frac{a}{d}, \frac{b}{d})$.

(b) Si $1 \sim \operatorname{pgcd}(a, b)$ et $a \mid y$ et $b \mid y$, alors $ab \mid y$.

(c) Un $\operatorname{ppcm}(a, b)$ existe et on a

$$\operatorname{ppcm}(a, b) \sim \frac{ab}{d} \text{ où } d \sim \operatorname{pgcd}(a, b).$$

Démonstration. (a) L'identité de Bézout divisée par d nous donne la relation

$$1 = r\frac{a}{d} + s\frac{b}{d}.$$

Donc tout diviseur de $\frac{a}{d}$ et $\frac{b}{d}$ divise aussi 1, montrant que 1 est un plus grand commun diviseur de $\frac{a}{d}$ et $\frac{b}{d}$.
(b) On part de l'identité de Bézout

$$1 = ra + sb.$$

Comme $a \mid y$, il existe $u \in A$ tel que $y = ua$. Multiplier la dernière égalité par r donne

$$ry = ura = u(1 - sb) = u - sbu,$$

donc

$$u = ry + sbu.$$

Comme $b \mid y$, on obtient $b \mid u$, donc il existe $v \in A$ tel que $u = vb$. Alors, nous avons $y = ua = v(ab)$.
(c) Soit $x := \frac{ab}{d}$. Il suffit de vérifier la définition :
– $x = a\frac{b}{d}$, donc $a \mid x$.
– $x = b\frac{a}{d}$, donc $b \mid x$.
– Soit $y \in A$ tel que $a \mid y$ et $b \mid y$. Alors $\frac{a}{d} \mid \frac{y}{d}$ et $\frac{b}{d} \mid \frac{y}{d}$. Par (a) nous avons $1 \sim \operatorname{pgcd}(\frac{a}{d}, \frac{b}{d})$. Utilisant (b) on en conclut $\frac{ab}{dd} \mid \frac{y}{d}$, donc $x = \frac{ab}{d} \mid y$.

□

Définition 5.12. *Soit A un anneau commutatif.*
– *Soient $a_1, \ldots, a_n \in A$. On note $(a_1, \ldots, a_n)$* l'idéal engendré par *$a_1, \ldots, a_n$:*

$$(a_1, \ldots, a_n) := Aa_1 + \cdots + Aa_n := \left\{ \sum_{i=1}^{n} r_i a_i \mid r_1, \ldots, r_n \in A \right\}.$$

– *Un idéal $I \trianglelefteq A$ est appelé* principal *s'il existe $a \in A$ tel que $I = (a)$.*
– *Un anneau intègre A est appelé* anneau principal *si tout idéal de A est un idéal principal.*

Exemple 5.13. – *Soit $n \in \mathbb{Z}$. Alors $n\mathbb{Z} = (n) = \{nm \mid m \in \mathbb{Z}\}$ est un idéal principal de $\mathbb{Z}$.*
– *Dans $\mathbb{Z}$ nous avons l'égalité $(2,3) = (1) = \mathbb{Z}$.*
Raison : « $\subseteq$ » est clair. « $\supseteq$ » : $1 = 3 - 2 \in (2,3)$.
– *$(2, X) \trianglelefteq \mathbb{Z}[X]$ n'est pas un idéal principal (Exercice).*

Lemme 5.14. *Soient A un anneau et $a, b \in A$.*

(a) $(a) \subseteq (b) \Leftrightarrow b \mid a$

(b) $(a) = (b) \Leftrightarrow a \sim b$ *(a et b sont associés)*

Démonstration. (a) Si $(a) \subseteq (b)$, alors il existe $c \in A$ tel que $a = cb$, alors $b \mid a$. Si $b \mid a$, alors il existe $c \in A$ tel que $a = cb$, alors $(a) \subseteq (b)$.
(b) Par (a), $(a) = (b)$ équivaut à ($a \mid b$ et $b \mid a$). Donc $a \sim b$. Si $a \sim b$, alors il existe une unité $u \in A^\times$ tel que $a = ub$, alors $(a) = (ub) = (b)$. □

Théorème 5.15. *Tout anneau euclidien est principal.*

Démonstration. Soient A un anneau euclidien (pour δ) et $I \trianglelefteq A$ un idéal. Nous allons montrer que I est un idéal principal. Si $I = \{0\}$, on a $I = (0)$, et I est principal (0 est le générateur).
Supposons donc $I \neq (0)$. Alors, l'ensemble

$$\{\delta(i) \mid i \in I, i \neq 0\} \subseteq \mathbb{N}$$

est non vide et possède donc un plus petit élément $\delta(a)$ pour un $0 \neq a \in I$. Comme $a \in I$, on a l'inclusion $(a) \subseteq I$. Nous allons démontrer l'autre.
Soit $x \in I$. La division euclidienne donne

$$x = qa + r \text{ où } q, r \in A \text{ tels que } \big(r = 0 \text{ ou } \delta(r) < \delta(a)\big).$$

Mais, $r \in I$ car $r = x - qa \in I$. Alors, soit $r = 0$, soit $\delta(r) \geq \delta(a)$. Comme la dernière possibilité est exclue, on a $r = 0$, donc $x = qa \in (a)$. Cela montre $I \subseteq (a)$, donc $I = (a)$ est un idéal principal. □

Exemple 5.16. – *$\mathbb{Z}$ est un anneau principal.*
– *$K[X]$ est un anneau principal si K est un corps.*
– *Tout corps est un anneau principal. En fait, tout idéal $\{0\} \neq I \lhd K$ est égal à $(1) = K$.*
Raison : Soit $0 \neq i \in I$. Comme K est un corps, i possède un inverse i^{-1}. Donc $1 = i^{-1}i \in I$, alors $(1) \subseteq I$, donc $(1) = I$.
– *$\mathbb{Z}[X]$ n'est pas un anneau principal car par exemple $(2, X)$ n'est pas un idéal principal.*

Proposition 5.17. *Soient A un anneau principal et $a, b, d, m \in A$.*

(a) $d \sim \operatorname{pgcd}(a,b) \Leftrightarrow (d) = (a,b)$.

(b) $m \sim \operatorname{ppcm}(a,b) \Leftrightarrow (m) = (a) \cap (b)$.

Démonstration. (a) « $\Rightarrow$ » : Comme d est un $\operatorname{pgcd}(a,b)$ il existe $r, s \in A$ tels que $d = ra + sb$, donc $d \in (a,b)$ et alors $(d) \subseteq (a,b)$. Comme $d \mid a$, on a que $a \in (d)$. Comme $d \mid b$, on a aussi $b \in (d)$, donc $(a,b) \subseteq (d)$, alors $(d) = (a,b)$.
« $\Leftarrow$ » : Comme $a, b \in (d)$ on a $d \mid a$ et $d \mid b$. Cela montre que d est un diviseur commun de a et b. Comme $(d) = (a,b)$ il existe $r, s \in A$ tels que $d = ra + sb$. Donc tout diviseur commun de a et b doit diviser d. Donc par définition d est un $\operatorname{pgcd}(a,b)$.
(b) La vérification pour le ppcm est très similaire à celle pour le pgcd. □

6 Anneaux factoriels

Dans la définition 5.13 d'Algèbre 1 nous avons défini un nombre premier comme un $p \in \mathbb{Z}_{\geq 2}$ dont les seuls diviseurs positifs sont 1 et p. Cela est équivalent à ce que p ne s'écrive pas comme produit $p = ab$ sauf si $a \in \{1, -1\} = \mathbb{Z}^\times$ ou $b \in \{1, -1\} = \mathbb{Z}^\times$. On pourrait alors dire (et on le dira aussi – voir la prochaine définition) que p est irréductible dans le sens qu'il ne se factorise pas de façon non triviale.
Nous avons aussi donné la caractérisation suivante qu'un $p \in \mathbb{Z}_{\geq 2}$ est un nombre premier dans le corollaire 5.32 d'Algèbre 1 :

p est premier $\Leftrightarrow$ si p divise un produit ab avec $a, b \in \mathbb{Z}$, alors $p \mid a$ ou $p \mid b$.

Nous allons utiliser cette caractérisation comme notre définition d'élément premier dans un anneau intègre quelconque.

Définition 6.1. *Soit A un anneau intègre et $0 \neq p \in A \setminus A^\times$.*
– *p est dit* irréductible *si l'assertion suivante est vraie :*

Si $p = ab$ avec $a, b \in A$, alors $a \in A^\times$ ou $b \in A^\times$.

– *p est dit* (élément) premier *si l'assertion suivante est vraie :*

Si p divise un produit ab avec $a, b \in A$, alors $p \mid a$ ou $p \mid b$.

Remarque 6.2.
– ***Par définition** une unité (c'est-à-dire un élément de $A^\times$) n'est ni premier ni irréductible. Ainsi, par exemple, 1 et -1 ne sont jamais ni premier ni irréductible.*
– *On définit ci-dessus deux notions à priori différentes : élément premier et élément irréductible. Dans certains anneaux (voire plus bas), ces deux notions sont les mêmes, mais **pas toujours**.*

Exemple 6.3.
– *Soit $u \in A^\times$ une unité. Si $0 \neq p \in A \setminus A^\times$ est premier, alors up est aussi premier. Si $0 \neq p \in A \setminus A^\times$ est irréductible, alors up est aussi irréductible.*
– *En Algèbre 1 nous avons donc vu que pour $n \in \mathbb{Z}_{\geq 2}$ on a l'équivalence*

$$n \text{ est premier } \Leftrightarrow n \text{ est irréductible.}$$

Nous allons redémontrer cette équivalence dans le contexte des anneaux euclidiens tout de suite. Pour $A = \mathbb{Z}$ et $0 \neq n \in \mathbb{Z} \setminus \{-1, 1\} = \mathbb{Z} \setminus \mathbb{Z}^\times$, on a que n est premier si et seulement si $|n|$ est un nombre premier (dans le sens d'Algèbre 1). Autrement dit, si $n \in \mathbb{Z}_{\geq 2}$ est un nombre premier, alors n et $-n$ sont des éléments premiers de l'anneau $\mathbb{Z}$.

D'abord un petit lemme.

Lemme 6.4. *Soit A un anneau intègre et $0 \neq p \in A \setminus A^\times$ premier. Si p divise un produit $a_1 a_2 \cdots a_n$ (avec $a_1, \ldots, a_n \in A$ et $n \in \mathbb{N}$), alors il existe $i \in \{1, \ldots, n\}$ tel que $p \mid a_i$.*

Démonstration. C'est une récurrence simple. Pour $n = 1$, l'assertion est triviale. Pour $n = 2$ c'est précisement la définition. Supposons le résultat démontré pour $n - 1 \geq 1$. Du fait que p divise $(a_1 \ldots a_{n-1}) \cdot a_n$ on conclut par la définition $p \mid a_1 \ldots a_{n-1}$ ou $p \mid a_n$. Dans le dernier cas nous avons terminé ($i = n$) ; dans le premier cas, par l'hypothèse de récurrence il existe $i \in \{1, \ldots, n-1\}$ tel que $p \mid a_i$ et nous avons aussi terminé. □

Dans l'exemple de $\mathbb{Z}$ nous avons vu que les éléments premiers et les éléments irréductibles sont les mêmes. En général cela n'est pas vrai, mais nous avons toujours l'implication que tout élément premier est irréductible :

Proposition 6.5. *Soit A un anneau intègre et $0 \neq p \in A \setminus A^\times$ premier. Alors p est irréductible.*

Démonstration. Soient $a, b \in A$ tels que $p = ab$. Cela implique que p divise ab. Comme p est premier, par définition $p \mid a$ ou $p \mid b$. Quitte à échanger a et b, sans perte de généralité nous supposons $p \mid a$. Donc il existe $c \in A$ tel que $a = pc$. Nous obtenons $p = ab = pbc$, alors $0 = p(1 - bc)$. Comme A est intègre, on a $1 = bc$, alors $b \in A^\times$. Nous avons donc vérifié que p est irréductible. □

Dans un anneau principal nous avons l'équivalence de « premier » et « irréductible » :

Proposition 6.6. *Soit A un anneau principal et $0 \neq p \in A \setminus A^\times$. Alors*

$$p \text{ est premier } \Leftrightarrow p \text{ est irréductible.}$$

Démonstration.
« $\Rightarrow$ » : Proposition 6.5.
« $\Leftarrow$ » : Soient $a, b \in A$ tel que $p \mid ab$. Il existe $c \in A$ tel que $ab = pc$. Supposons que p ne divise pas a (sinon, nous avons déjà terminé). Il existe $m \in A$ tel que

$$(p) \subsetneq (p, a) = (m),$$

où nous avons utilisé le fait que A est principal en écrivant l'idéal (p, a) comme idéal principal. Donc $p \in (m)$ et alors $m \mid p$: il existe $n \in A$ tel que $p = mn$. Maintenant nous utilisons que p est irréductible : $m \in A^\times$ ou $n \in A^\times$. Si $n \in A^\times$, alors $(p) = (m)$ ce qui est exclu. Donc $m \in A^\times$. Alors $1 = m^{-1}m \in (m) = (p, a)$. Il existe donc $r, s \in A$ tels que $1 = rp + sa$. On multiplie cette égalité par b pour obtenir $b = prb + abs = prb + pcs = p(rb + cs)$. Donc $p \mid b$, comme il fallait montrer pour conclure que p est premier. □

Un des théorèmes principaux sur $\mathbb{Z}$ démontré en Algèbre 1 est le « théorème principal de la théorie élémentaire des nombres » : Tout entier $0 \neq n \in \mathbb{Z}$ s'écrit de façon unique (à numérotation près) comme produit fini de nombres premiers.
Nous allons retrouver ce théorème ici dans la formulation « $\mathbb{Z}$ est un anneau factoriel » qui sera une conséquence de : « tout anneau principal est un anneau factoriel ». Pour obtenir ce résultat il nous faut quelques préparations. D'abord la définition.

Définition 6.7. *Un anneau intègre A est appelé* anneau factoriel *si tout $0 \neq a \in A \setminus A^\times$ s'écrit comme produit fini d'éléments premiers, c'est-à-dire qu'il existe $n \in \mathbb{N}$ et $p_1, \ldots, p_n \in A \setminus A^\times$ premiers tels que $a = p_1 \cdot p_2 \cdots p_n$.*

Proposition 6.8. *Soit A un anneau factoriel et $0 \neq p \in A \setminus A^\times$. Alors*

$$p \text{ est premier } \Leftrightarrow p \text{ est irréductible.}$$

Démonstration.
« $\Rightarrow$ » : Proposition 6.5.
« $\Leftarrow$ » : Par la définition des anneaux factoriels, il existe $n \in \mathbb{N}$ et $p_1, \dots, p_n \in A \setminus A^\times$ premiers tels que $p = p_1 \cdot p_2 \cdots p_n$. Le fait que p est irréductible implique $n = 1$ et $p = p_1$, donc p est premier. □

Proposition 6.9. *Soit A un anneau intègre. Soit $\mathbb{P}$ un ensemble de représentants des éléments irréductibles de A à association près. Les assertions suivantes sont équivalentes :*

(i) A est factoriel.

(ii) Pour tout $0 \neq a \in A$ il existe une unique unité $u \in A^\times$, un unique $n \in \mathbb{N}_{\geq 0}$ et des uniques $p_1, \dots, p_n \in \mathbb{P}$ (à l'ordre près) tels que

$$a = u \cdot p_1 \cdot p_2 \cdots p_n.$$

Démonstration.
« (i) $\Rightarrow$ (ii) » : Pour cette partie nous utiliserons qu'un élément est irréductible si et seulement s'il est premier (proposition 6.8).
Existence : Soit $0 \neq a \in A$. Comme on suppose donc que A est factoriel, il existe $n \in \mathbb{N}_{\geq 0}$ et des éléments premiers $p'_1, \dots, p'_n$ tels que $a = p'_1 \cdot p'_2 \cdots p'_n$. Comme tout élément premier est irréductible (proposition 6.5) et $\mathbb{P}$ est un ensemble de représentants des éléments irréductibles à association près, il existe $u_1, \dots, u_n \in A^\times$ tels que $p_i := u_i p'_i \in \mathbb{P}$. Posant $u = u_1^{-1} \cdot u_2^{-1} \cdots u_n^{-1} \in A^\times$ on obtient $a = u \cdot p_1 \cdot p_2 \cdots p_n$ qui est de la forme requise.
Unicité : On fait une récurrence. Nous démontrons l'unicité pour les $0 \neq a \in A$ pouvant s'écrire avec au maximum n éléments de $\mathbb{P}$: $a = u \cdot p_1 \cdot p_2 \cdots p_n$. On suppose donc donnée une deuxième écriture de cette forme :

$$a = u \cdot p_1 \cdot p_2 \cdots p_n = v \cdot q_1 \cdot q_2 \cdots q_m$$

avec $u, v \in A^\times$, $n, m \in \mathbb{N}$ et $p_1, \dots, p_n, q_1, \dots, q_m \in \mathbb{P}$.
Cas $n = 0$: On a alors $a = u = v \cdot q_1 \cdot q_2 \cdots q_m$. Comme un nombre premier n'est pas une unité, on a $m = 0$ et l'unicité est claire.
Supposons l'assertion démontrée pour $n - 1 \geq 0$, on va la démontrer pour n. Comme p_n divise $u \cdot p_1 \cdot p_2 \cdots p_n$, il s'en suit que p_n divise $v \cdot q_1 \cdot q_2 \cdots q_m$. Maintenant on utilise que p_n est un nombre premier et le lemme 6.4 pour obtenir un $j \in \{1, \dots, m\}$ tel que $p_n \mid q_j$. Comme q_j est irréductible, on a $p_n \sim q_j$, donc $p_n = q_j$ car $p_n, q_j \in \mathbb{P}$. On considère maintenant

$$\frac{a}{p_n} = u \cdot p_1 \cdot p_2 \cdots p_{n-1} = v \cdot q_1 \cdot q_2 \cdots q_{j-1} \cdot q_{j+1} \cdots q_m.$$

Cela nous permet d'utiliser l'hypothèse de récurrence qui nous donne $n - 1 = m - 1$ (donc $n = m$), $u = v$ et une bijection $\sigma' : \{1, \dots, n-1\} \to \{1, \dots, m\} \setminus \{j\}$ telle que $p_i = q_{\sigma'(i)}$ pour tout $i \in \{1, \dots, n-1\}$. Nous définissons la bijection $\sigma : \{1, \dots, n\} \to \{1, \dots, m\}$ par la règle $\sigma(n) = j$ et $\sigma(i) = \sigma'(i)$ pour $1 \leq i \leq n-1$ qui possède la propriété, $p_i = q_{\sigma(i)}$ pour tout $i \in \{1, \dots, n\}$. Cela achève la démonstration de l'unicité.
« (ii) $\Rightarrow$ (i) » : Il suffit de démontrer que tout élément irréductible $0 \neq p \in A \setminus A^\times$ est premier. Quitte à multiplier p par une unité (ce qui ne change pas la propriété d'être premier ou non) on peut supposer $p \in \mathbb{P}$. Soient donc $g, h \in A$ deux éléments tels que $p \mid gh$. Il existe alors $r \in A$ tel que $pr = gh$.

On a $g = u \cdot p_1 \cdots p_n$ et $h = v \cdot q_1 \cdots q_s$ et $r = w \cdot \ell_1 \cdots \ell_t$ avec $u, v, w \in A^\times$, $n, s, t \in \mathbb{N}$ et $p_1, \ldots, p_n, q_1, \ldots, q_s, \ell_1, \ldots, \ell_t \in \mathbb{P}$. L'égalité

$$pr = w \cdot p \cdot \ell_1 \cdots \ell_t = (u \cdot v) \cdot p_1 \cdots p_n \cdot q_1 \cdots q_s = gh$$

combinée avec l'unicité de l'écriture de (ii) implique que p est égal à p_i pour un $i \in \{1, \ldots, n\}$ ou à q_j pour un $j \in \{1, \ldots, s\}$. Donc, p divise g ou p divise h. Cela montre que p est premier. □

Lemme 6.10. *Soient A un anneau principal et $a_n \in A$ pour $n \in \mathbb{N}$ tels que*

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots \subseteq (a_n) \subseteq (a_{n+1}) \subseteq \ldots$$

Alors il existe $N \in \mathbb{N}$ tel que pour tout $n \geq N$ on a $(a_n) = (a_N)$. On dit que la chaîne d'idéaux devient stationnaire. En langage de l'algèbre commutatif on dit que tout anneau principal est « noethérien ».

Démonstration. Soit $I = \bigcup_{n \in \mathbb{N}} (a_n)$.
Nous montrons d'abord que I est un idéal de A : Soient $x, y \in I$ et $r \in A$. Il existe $i, j \in \mathbb{N}$ tel que $x \in (a_i)$ et $y \in (a_j)$. Soit $k = \max(i, j)$. Alors $x, y \in (a_k)$. Donc $x - y \in (a_k) \subseteq I$ et $rx \in (a_k) \subseteq I$, montrant $I \trianglelefteq A$.
Comme A est principal, il existe $a \in A$ tel que $I = (a)$. Comme I est la réunion de tous les (a_n) il existe $N \in \mathbb{N}$ tel que $a \in (a_N)$. Alors

$$I = (a) \subseteq (a_N) \subseteq (a_{N+1}) \subseteq (a_{N+2}) \subseteq \cdots \subseteq I$$

et la preuve est terminée. □

Lemme 6.11. *Soit A un anneau principal. Alors tout $0 \neq a \in A \setminus A^\times$ est divisible par un élément irréductible dans A.*

Démonstration. Supposons que c'est faux et que a n'est pas divisible par un élément irréductible (en particulier, a n'est pas lui-même irréductible).
– Alors $a = a_1 b_1$ avec $a_1, b_1 \in A \setminus A^\times$ qui ne sont pas divisibles par un élément irréductible. On a $(a) \subsetneq (a_1)$.
– Alors $a_1 = a_2 b_2$ avec $a_2, b_2 \in A \setminus A^\times$ qui ne sont pas divisibles par un élément irréductible. On a $(a) \subsetneq (a_1) \subsetneq (a_2)$.
– Alors $a_2 = a_3 b_3$ avec $a_3, b_3 \in A \setminus A^\times$ qui ne sont pas divisibles par un élément irréductible. On a $(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq (a_3)$.
– ...
Continuant ainsi nous obtenons une suite croissante d'idéaux qui n'existe pas par le lemme 6.10. □

Théorème 6.12. *Tout anneau principal est factoriel.*

Démonstration. La preuve est similaire à la preuve précédente. Par la proposition 6.6 et la définition d'anneau factoriel, il suffit de montrer que tout $0 \neq a \in A$ s'écrit comme produit fini d'éléments irréductibles.

– Si $a \notin A^\times$, par le lemme 6.11 il existe $0 \neq a_1 \in A \setminus A^\times$ irréductible et $b_1 \in A$ tels que $a = a_1 b_1$. Donc $(a) \subsetneq (b_1)$.
– Si $b_1 \notin A^\times$, par le lemme 6.11 il existe $0 \neq a_2 \in A \setminus A^\times$ irréductible et $b_2 \in A$ tels que $b_1 = a_2 b_2$. Donc $(a) \subsetneq (b_1) \subsetneq (b_2)$ et $a = a_1 a_2 b_2$.
– Si $b_2 \notin A^\times$, par le lemme 6.11 il existe $0 \neq a_3 \in A \setminus A^\times$ irréductible et $b_3 \in A$ tels que $b_2 = a_3 b_3$. Donc $(a) \subsetneq (b_1) \subsetneq (b_2) \subsetneq (b_3)$ et $a = a_1 a_2 a_3 b_3$.
– ...

Par le lemme 6.10, il existe $n \in \mathbb{N}$ tel que $b_n \in A^\times$. À ce moment-là on a $a = a_1 a_2 \cdots a_{n-1}(a_n b_n)$. La preuve est terminée car $a_n b_n$ est aussi irréductible. □

Corollaire 6.13. *Pour un anneau A nous avons les implications :*

$$A \text{ est euclidien } \Rightarrow A \text{ est principal } \Rightarrow A \text{ est factoriel } \Rightarrow A \text{ est intègre.}$$

Démonstration. Nous avons tout démontré dans les théorèmes 6.12 et 5.15. □

7 Compléments de la théorie des anneaux

Définition 7.1. *Soit A un anneau.*
– *Un idéal $I \lhd A$, $I \neq A$ est appelé* premier *si l'assertion suivante sur I est vraie :*

À chaque fois que $a \cdot b \in I$ avec $a, b \in A$, alors $a \in I$ ou $b \in I$.

– *Un idéal $I \lhd A$, $I \neq A$ est appelé* maximal *si le seul idéal $J \lhd A$ tel que $I \subsetneq J$ est $J = A$.*

Lemme 7.2. *Soit A un anneau. Alors : A est intègre $\Leftrightarrow (0)$ est un idéal premier.*

Démonstration. Exercice. □

La définition est motivée par l'interprétation suivante :

Proposition 7.3. *Soient A un anneau intègre et $0 \neq p \in A \setminus A^\times$.*

(a) $(p) \lhd A$ est (un idéal) premier $\Leftrightarrow$ p est (un élément) premier.

(b) $(p) \lhd A$ est (un idéal) maximal $\Rightarrow$ p est (un élément) irréductible.

Démonstration. (a) Il suffit de se rappeler : $p \mid ab \;\Leftrightarrow\; ab \in (p)$.
(b) Soit $p = ab$ avec $a, b \in A$. Donc $p \mid a$, donc $(p) \subseteq (a) \trianglelefteq A$. La maximalité de (p) implique : soit $(p) = (a)$ (dans ce cas $b \in A^\times$), soit $(a) = A$ (dans ce cas $a \in A^\times$). Alors p est irréductible. □

L'implication inverse de (b) n'est pas vraie en général, mais elle est valable dans les anneaux principaux :

Proposition 7.4. *Soient A un anneau principal et $0 \neq p \in A \setminus A^\times$. Alors :*
$(p) \lhd A$ est (un idéal) maximal $\Leftrightarrow$ p est (un élément) irréductible.

Démonstration. Par (b) de la proposition 7.3 il suffit de démontrer « $\Leftarrow$ ». Soit p donc irréductible et soit $J \lhd A$ un idéal tel que $(p) \subseteq J$ et $J \neq A$. Comme l'anneau est principal, on a $J = (j)$ pour un $j \in J$. Comme J n'est pas A, l'élément j n'est pas inversible dans A. L'inclusion $(p) \subseteq (j)$ implique $j \mid p$, donc $p = jb$ pour un $b \in A$. Comme p est irréductible, alors $b \in A^\times$ et alors $(p) = (j) = J$, montrant que (p) est un idéal maximal. □

La théorie des idéaux premiers et maximaux dans un anneau principal est donc très simple :

Proposition 7.5. *Soit A un anneau principal.*

(a) Les idéaux premiers de A sont (0) et les idéaux principaux engendrés par les éléments premiers.

(b) On suppose ici que A n'est pas un corps. Les idéaux maximaux de A sont les idéaux principaux engendrés par les éléments premiers.

Démonstration. Tout idéal est principal et par la proposition 6.8 un élément $0 \neq p \in A \setminus A^\times$ est irréductible si et seulement s'il est premier. Les propositions 7.3(a) et 7.4 nous assurent des équivalences :

$$(p) \text{ premier } \Leftrightarrow p \text{ irréductible } \Leftrightarrow (p) \text{ maximal.}$$

Il suffit donc de regarder les idéaux (a) avec $a = 0$ ou $a \in A^\times$. Si $a \in A^\times$, alors $(a) = A$ et donc (a) ne peut ni être maximal ni premier car la définition exige $(a) \neq A$. Finalement on étudie $(0) = \{0\}$. C'est un idéal premier car A est intègre par le lemme 7.2. Si A n'est pas un corps, alors il existe $0 \neq a \in A \setminus A^\times$, donc $(0) \subsetneq (a) \subsetneq A$, alors (0) n'est pas maximal. □

Proposition 7.6. *Soient A un anneau et $I \lhd A$, $I \neq A$ un idéal.*

(a) I est premier $\Leftrightarrow$ A/I est intègre.

(b) I est maximal $\Leftrightarrow$ A/I est un corps.

(c) I est maximal $\Rightarrow$ I est premier.

Démonstration. (a) « $\Rightarrow$ » : Supposons $(a+I)(b+I) = 0+I$. Alors $ab + I = 0 + I$, donc $ab \in I$. Comme I est premier, $a \in I$ ou $b \in I$. En conséquence, $a + I = 0 + I$ ou $b + I = 0 + I$. Nous avons montré que le seul diviseur de zéro dans A/I est $0 + I$, alors, A/I est intègre.
« $\Leftarrow$ » : Supposons que $ab \in I$. Alors $0 + I = ab + I = (a + I)(b + I)$. Comme A/I est intègre, on a $a + I = 0 + I$ ou $b + I = 0 + I$, donc $a \in I$ ou $b \in I$. Cela montre que I est un idéal premier.
(b) « $\Rightarrow$ » : Soit $a + I \neq 0 + I$. On doit montrer que $a + I$ est inversible. Comme $a + I \neq 0 + I$, on a $a \notin I$. Soit $J = (I, a)$, l'idéal engendré par a et I. Donc $I \subsetneq (I, a)$. La maximalité de I implique $J = A$. Donc $1 \in J$, donc $1 = i + ra$ pour un $i \in I$ et un $r \in R$. En conséquence $1 + I = ra + I = (a + I)(r + I)$, et nous avons trouvé l'inverse.
« $\Leftarrow$ » : On veut montrer que I est maximal. Soit donc $J \trianglelefteq A$ un idéal tel que $I \subsetneq J$. Soit $a \in J \setminus I$. Comme $a \notin I$, l'élément $a + I$ de A/I possède un inverse $1 + I = (a + I)(b + I)$. La relation $1 \in ab + I \subseteq J$ montre $J = A$ et donc la maximalité de I.
(c) I maximal $\Rightarrow$ A/I corps $\Rightarrow$ A/I anneau intègre $\Rightarrow$ I est premier. □

En Algèbre 1 nous avons introduit les ensembles d'un point de vue intuitif et non rigoureux. Un traitement strict ne peut se faire que dans un cours de logique à un moment plus avancé (un tel cours n'est pas offert à l'UL en ce moment – vous pouvez regarder des livres pour plus de détails). Dans la théorie des ensembles il y a un axiome important : « l'axiome du choix ».[1] Dans la théorie des ensembles on montre le « lemme de Zorn » qui dit que l'axiome du choix est équivalent à l'assertion suivante.

[1] L'axiome du choix : Soit X un ensemble dont les éléments sont des ensembles non vides. Alors il existe une fonction f définie sur X qui à chaque $M \in X$ associe un élément de M. Une telle fonction est appelée « fonction du choix ».

Axiome 7.7 (Lemme de Zorn)**.** *Soit S un ensemble non-vide et $\leq$ une relation d'ordre sur S.*[2] *On fait l'hypothèse suivante : Tout sous-ensemble $T \subseteq S$ qui est totalement ordonné*[3] *possède un majorant.*[4] *Alors, S contient un élément maximal.*[5]

Pour montrer comment appliquer le lemme de Zorn nous démontrons d'abord que tout espace vectoriel possède une base. Si vous avez vu cette assertion dans votre cours d'algèbre linéaire, alors c'était pour des espaces vectoriels de dimension finie car le cas général est en fait équivalent à l'axiome du choix (et donc au lemme de Zorn).

Proposition 7.8. *Soit K un corps et $V \neq \{0\}$ un K-espace vectoriel. Alors, V possède une K-base.*

Démonstration. On rappelle quelques notions d'algèbre linéaire. Un sous-ensemble fini $G \subseteq V$ est appelé *K-linéairement indépendant* si la seule combinaison linéaire $0 = \sum_{g \in G} a_g g$ avec $a_g \in K$ est celle où $a_g = 0$ pour tout $g \in G$. Plus généralement, un sous-ensemble pas nécessairement fini $G \subseteq V$ est appelé *K-linéairement indépendant* si tout sous-ensemble fini $H \subseteq G$ est K-linéairement indépendant. Un sous-ensemble $G \subseteq V$ est appelé une *K-base* s'il est K-linéairement indépendant et engendre V.[6]
On veut utiliser le lemme de Zorn 7.7. Soit

$$S := \{G \subseteq V \text{ sous-ensemble} \mid G \text{ est } K\text{-linéairement indépendant } \}.$$

L'ensemble S est non-vide car $G = \{v\}$ est K-linéairement indépendant pour tout $0 \neq v \in V$. L'inclusion d'ensembles « $\subseteq$ » définit une relation d'ordre sur S (c'est évident – voir Algèbre 1).
On vérifie que l'hypothèse du lemme de Zorn est satisfaite : Soit $T \subseteq S$ un sous-ensemble totalement ordonné. On doit produire un majorant $E \in S$ pour T. On pose $E := \bigcup_{G \in T} G$. Il est clair que $G \subseteq E$ pour tout $G \in T$. Il faut montrer que $E \in S$, donc que E est K-linéairement indépendant. Soit $H \subseteq E$ un sous-ensemble de cardinal n. On montre par récurrence en n qu'il existe $G \in T$ tel que $H \subseteq G$. L'assertion est claire pour $n = 1$. Supposons-la démontrée pour $n - 1$ et écrivons $H = H' \sqcup \{h\}$. Il existe $G', G \in T$ tels que $H' \subseteq G'$ (par l'hypothèse de récurrence car le cardinal de H' est $n - 1$) et $h \in G$ (par le cas $n = 1$). Par le fait que T est totalement ordonné, on a $G \subseteq G'$ ou $G' \subseteq G$. Dans les deux cas on obtient que H est un sous-ensemble de G ou de G'. Comme H est un sous-ensemble fini d'un ensemble qui est K-linéairement indépendant, H l'est aussi. Donc, E est K-linéairement indépendant.
Le lemme de Zorn nous donne un élément maximal $B \in S$. On montre que B est une K-base de V. En tant qu'élément de S, B est K-linéairement indépendant. Il faut démontrer que B engendre V. Supposons que cela ne soit pas le cas et prenons $v \in V$ qui ne s'écrit pas comme combinaison K-linéaire des éléments dans B. Alors l'ensemble $G := B \cup \{v\}$ est aussi K-linéairement indépendant, car toute

[2] On rappelle que par définition les trois points suivants sont satisfaits :
- $s \leq s$ pour tout $s \in S$.
- Si $s \leq t$ et $t \leq s$ pour $s, t \in S$, alors $s = t$.
- Si $s \leq t$ et $t \leq u$ pour $s, t, u \in S$, alors $s \leq u$.

[3] T est totalement ordonné si T est ordonné et pour tout couple $s, t \in T$ on a $s \leq t$ ou $t \leq s$.
[4] $g \in S$ est un majorant pour T si $t \leq g$ pour tout $t \in T$.
[5] $m \in S$ est maximal si pour tout $s \in S$ tel que $m \leq s$ on a $m = s$.
[6] C'est-à-dire : tout élément $v \in V$ s'écrit comme $v = \sum_{i=1}^{n} a_i g_i$ avec $n \in \mathbb{N}$, $a_1, \ldots, a_n \in K$ et $g_1, \ldots, g_n \in G$.

combinaison K-linéaire $0 = av + \sum_{i=1}^{n} a_i b_i$ avec $n \in \mathbb{N}$, $a, a_1, \ldots, a_n \in K$ et $b_1, \ldots, b_n \in B$ avec $a \neq 0$ donnerait la contradiction $v = \sum_{i=1}^{n} \frac{-a_i}{a} b_i$ (noter que $a = 0$ correspond à une combinaison K-linéaire dans B qui est K-linéairement indépendant). Mais, $B \subsetneq G \in S$ contredit la maximalité de B. □

Dans cette section nous nous intéressons à l'existence des idéaux maximaux. Pour la démontrer nous avons aussi besoin du lemme de Zorn.

Proposition 7.9. *Soit $A \neq \{0\}$ un anneau. Alors A possède un idéal maximal.*

Démonstration. On utilise encore le lemme de Zorn 7.7. Soit

$$S := \{I \lhd A \text{ idéal} \mid I \neq A\}.$$

L'ensemble S est non-vide car $(0) \in S$. L'inclusion d'ensembles « $\subseteq$ » définit encore une relation d'ordre sur S.
On vérifie que l'hypothèse du lemme de Zorn est satisfaite : Soit $T \subseteq S$ un sous-ensemble totalement ordonné. On doit produire un majorant $E \in S$ pour T. On pose encore $E = \bigcup_{I \in T} I$. Il faut démontrer que E est un idéal de A différent de A. Soient $x, y \in E$ et $a \in A$. Il existe $I_x, I_y \in T$ tels que $x \in I_x$ et $y \in I_y$. Comme T est totalement ordonné, on soit $I_x \subseteq I_y$ ou $I_y \subseteq I_x$. Soit $I = I_x \cup I_y$, alors $I = I_x$ ou $I = I_y$. Alors $x, y \in I$. Comme c'est un idéal, on a $x - y \in I \subseteq E$ et $ax \in I \subseteq E$. Cela montre que E est un idéal. Pour montrer $E \neq A$ on suppose le contraire. Dans ce cas $1 \in E$. Alors il existe $I \in T$ tel que $1 \in I$. Mais cela implique $I = A$, une contradiction. Donc E est bien un majorant pour T.
Le lemme de Zorn nous produit un élément maximal $\mathfrak{m} \in S$. Par définition c'est un idéal maximal. □

Corollaire 7.10. *Soit $A \neq \{0\}$ un anneau.*

(a) Tout idéal $I \lhd A$, $I \neq A$ est contenu dans un idéal maximal.

(b) Tout $x \in A \setminus A^\times$ est contenu dans un idéal maximal.

Démonstration. (a) Soit $\pi : A \twoheadrightarrow A/I$ la projection naturelle qui envoie a sur $a + I$. Par la proposition 7.9 il existe un idéal maximal $\mathfrak{m} \in A/I$. Soit $M := \pi^{-1}(\mathfrak{m})$ l'image réciproque de $\mathfrak{m}$ par π. Autrement dit, M est le noyau de l'homomorphisme d'anneaux composé $\varphi : A \xrightarrow{\pi} A/I \xrightarrow{\text{proj. naturelle}} (A/I)/\mathfrak{m}$. Comme cet homomorphisme est surjectif, le théorème d'isomorphisme donne l'isomorphisme d'anneaux $\overline{\varphi} : A/M \to (A/I)/\mathfrak{m}$. Puisque $\mathfrak{m}$ est maximal, par la proposition 7.6 $(A/I)/\mathfrak{m}$ est un corps, donc A/M est un corps, donc M est maximal.
(b) Utiliser (a) avec $I = (x)$. □

On finit cette section par la définition du corps des fractions d'un anneau intègre qui généralise de façon directe la construction des nombres rationnels donnée en Algèbre 1 (définiton 6.1 et proposition 6.2).

Définition-Lemme 7.11. *Soit A un anneau intègre. Sur $A \times (A \setminus \{0\})$ on définit une relation*

$$(a, x) \sim (b, y) \Leftrightarrow ay = bx.$$

C'est une relation d'équivalence.
La classe de (a, x) *est formée de tous les* (b, y) *tel que* $ay = bx$*, ce qui justifie la notation* $\frac{a}{x}$ *pour la classe* $\overline{(a, x)}$*.*
L'ensemble quotient est noté $\mathrm{Frac}(A)$*.*

Démonstration. Exercice. □

Proposition 7.12. *Soit* $K := \mathrm{Frac}(A)$ *l'ensemble quotient de la définition-lemme 7.11.*

(a) Les deux applications

$$+ : K \times K \to K, \quad \frac{a}{x} + \frac{b}{y} := \frac{ay + bx}{xy}$$

et

$$\cdot : K \times K \to K, \quad \frac{a}{x} \cdot \frac{b}{y} := \frac{ab}{xy}$$

sont bien définies, c'est-à-dire que leurs définitions ne dépendent pas des choix des représentants (a, x) *et* (b, y) *des classes* $\frac{a}{x}$ *et* $\frac{b}{y}$*.*

(b) $(K, +, \cdot, \frac{0}{1}, \frac{1}{1})$ *est un corps.*

(c) L'application

$$\iota : A \to K, \quad a \mapsto \frac{a}{1}$$

est injective et on a $\iota(a + b) = \iota(a) + \iota(b)$ *et* $\iota(a \cdot b) = \iota(a) \cdot \iota(b)$ *pour tous* $a, b \in K$*.*

Démonstration. Exercice. □

Exercices : Algèbre 2

Semestre d'été 2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David

Feuille 1

19/02/2013

Ces exercices sont à rendre le 26/02/2013 au début du cours. L'un/une d'entre vous présentera un des exercices lors du cours du 05/03/2013.

---

1. Soit $(K, +, \cdot, 0, 1)$ un corps (commutatif !). On écrit $\mathrm{Mat}_n(K)$ pour les matrices d'ordre n (pour $n \in \mathbb{N}$) à coefficients dans K.
   (a) Démontrer que $(\mathrm{Mat}_n(K), +, ., \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix})$ est un K-espace vectoriel.
   (b) Donner une base de cet espace vectoriel.
   (c) On note

   $$\mathrm{GL}_n(K) := \{M \in \mathrm{Mat}_n(K) \mid M \text{ est inversible } \} = \{M \in \mathrm{Mat}_n(K) \mid \det(M) \neq 0\},$$

   appelé *le groupe général linéaire*.
   Pour $n = 2$ et $K = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ calculer le cardinal du groupe $\mathrm{GL}_2(\mathbb{F}_2)$.
   Est-ce que c'est un groupe abélien ?
2. Soit $n \in \mathbb{N}_{>0}$. Démontrer que l'application $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $a \mapsto \overline{a} = a + n\mathbb{Z}$, est un homomorphisme d'anneaux.
3. Propriétés des noyaux et des images :
   (a) Soit $\varphi : G \to H$ un homomorphisme de groupes.
   Montrez que $\ker(\varphi)$ est un sous-groupe normal de G et que $\mathrm{im}(\varphi)$ est un sous-groupe de H.
   Donnez un exemple où $\mathrm{im}(\varphi)$ est normal et un exemple où $\mathrm{im}(\varphi)$ n'est pas normal.
   (b) Soit $\varphi : A \to B$ un homomorphisme d'anneaux.
   Montrez que $\ker(\varphi)$ est un idéal de A et que $\mathrm{im}(\varphi)$ est un sous-anneau de B.
   (c) Soit K un corps (commutatif !) et $\varphi : V \to W$ un homomorphisme de K-espaces vectoriels.
   Démontrer que $\ker(\varphi)$ est un sous-K-espace vectoriel de V et que $\mathrm{im}(\varphi)$ est un sous-K-espace vectoriel de W.

À propos. Le concept moderne et abstrait de groupe se développa à travers différents champs des mathématiques.

La motivation originelle de la théorie des groupes fut la recherche des solutions des équations polynomiales de degré supérieur à quatre. Au XIXe siècle, le mathématicien français Évariste Galois, développant des travaux précédents de Paolo Ruffini et Joseph-Louis Lagrange, donna un critère de résolubilité d'équations polynomiales particulières en termes de groupe de symétrie de leurs racines. Les éléments d'un tel groupe (appelé groupe de Galois) correspondent à certaines permutations des racines. Les idées de Galois furent méconnues par ses contemporains et publiées seulement à titre posthume. Des groupes

de permutations plus généraux furent étudiés par Augustin Louis Cauchy. Arthur Cayley, dans un article de 1854, donna la première définition abstraite d'un groupe fini.

La géométrie fut le second domaine dans lequel les groupes furent systématiquement utilisés, en particulier dans le programme d'Erlangen de Felix Klein, en 1872. Après que de nouvelles géométries, comme la géométrie hyperbolique et la géométrie projective, eurent émergé, Klein utilisa la théorie des groupes pour les organiser en un système cohérent. En prolongeant ces idées, Sophus Lie posa les fondations de l'étude des groupes de Lie en 1884.

Le troisième domaine qui contribua à la théorie des groupes fut la théorie des nombres. Certaines structures de groupe abélien ont été implicitement utilisées par Carl Friedrich Gauss dans ses Disquisitiones Arithmeticae (1798), et plus explicitement par Leopold Kronecker. En 1847, Ernst Kummer mena les premières tentatives de preuve du dernier théorème de Fermat à leur point culminant en développant une factorisation des groupes en nombres premiers.

La convergence de ces différentes sources en une théorie des groupes uniforme commença avec le Traité des substitutions et des équations algébriques (1870) de Camille Jordan. Walther von Dyck (1882) donna le premier énoncé moderne de la définition d'un groupe abstrait. Durant le XXe siècle, les groupes gagnèrent une grande reconnaissance avec les travaux de Ferdinand Georg Frobenius et William Burnside, qui travaillèrent sur la théorie des représentations d'un groupe fini, la théorie des représentations modulaires de Richard Brauer et les articles de Issai Schur. La théorie des groupes de Lie, et plus généralement des groupes localement compacts fut développée par Hermann Weyl, Élie Cartan et beaucoup d'autres. Son aspect algébrique, la théorie des groupes algébriques, fut tout d'abord formée par Claude Chevalley, à la fin des années 1930, puis par le travail essentiel d'Armand Borel et Jacques Tits.

Source : `http ://fr.wikipedia.org/wiki/Groupe_(mathématiques)`

Exercices : Algèbre 2

Semestre d'été 2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David

Feuille 2

26/02/2013

Ces exercices sont à rendre le 05/03/2013 au début du cours. L'un/une d'entre vous présentera un des exercices lors du cours du 12/03/2013.

---

1. Soient $n \in \mathbb{N}_{>0}$, $(K, +, \cdot, 0, 1)$ un corps (commutatif !) et $\varphi : K \to \mathrm{Mat}_n(K)$, $a \mapsto \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & a & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a \end{pmatrix}$.

   Démontrer que $(\mathrm{Mat}_n(K), \varphi)$ est une K-algèbre.

   Noter la correction dans la définition donnée au cours.

2. Soient $(A, +, \cdot, 0, 1)$ un anneau commutatif et $I \trianglelefteq A$ un idéal. Dans le cours nous avons démontré :

   Soient $a, b \in A$. *La <u>classe</u> $ab + I$ ne dépend que de la <u>classe</u> $a + I$ et de la <u>classe</u> $b + I$.*

   Ceci nous a permis de faire la définition $(a + I) \otimes (b + I) := ab + I$.

   Démontrer :

   (a) $(A/I, \oplus, \otimes, 0 + I, 1 + I)$ est un anneau commutatif.

   Indication : Vous pouvez (et devrez) utiliser que nous savons déjà que $(A/I, \oplus, 0+I)$ est un groupe abélien.

   (b) L'application « projection naturelle »

   $$\pi : A \to A/I, \quad a \mapsto a + I$$

   est un homomorphisme d'anneaux surjectif de noyau $\ker(\pi) = I$.

3. Soit A un anneau et $I \trianglelefteq A$ un idéal et $\pi : A \to A/I$ la projection naturelle de l'exercice précédent.

   Démontrer : L'application

   $$\Phi : \{\text{idéaux de } A/I\} \longrightarrow \{\text{idéaux de } A \text{ qui contiennent } I\},$$

   donnée par $J \mapsto \pi^{-1}(J)$ est bijective. L'inverse de Φ est $K \mapsto \pi(K)$.

   Indication : On peut utiliser les résultats de la proposition correspondante pour les groupes.

À propos. L'étude des corps et des anneaux trouve son origine dans l'école allemande du XIXe siècle. Elle est développée par les mathématiciens Kummer, Dedekind, Kronecker et Hilbert. Elle naît de l'étude des équations algébriques, des nombres algébriques et de la recherche d'une démonstration du grand théorème de Fermat. Elle conduira à un développement important de l'algèbre générale et de la géométrie algébrique.

Dans le Xe Supplément de sa seconde édition des Leçons sur la théorie des nombres de Dirichlet, en 1871, Dedekind considère, à côté de la notion de corps (Körper), l'anneau des entiers d'un corps de nombres algébriques ; il introduira un peu plus tard d'autres anneaux qu'il appelle ordres (Ordnung). Mais c'est David Hilbert qui emploie le terme d'anneau (Ring) pour définir ce qui est toujours à l'époque un anneau commutatif unitaire, dans son Rapport sur les nombres (Zahlbericht) de 1897 pour la Deutsche Mathematiker-Vereinigung.

Source : `http ://fr.wikipedia.org/wiki/Anneau_unitaire`

Exercices : Algèbre 2

Semestre d'été 2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David

Feuille 3

05/03/2013

Ces exercices sont à rendre le 12/03/2013 au début du cours. L'un/une d'entre vous présentera un des exercices lors du cours du 19/03/2013.

---

1. (a) Vérifier la construction de quotients d'espaces vectoriels, c'est-à-dire, démontrer la proposition 2.10 du cours.

   (b) Soit $V = \mathbb{R}^2$, le $\mathbb{R}$-espace vectoriel « standard » de dimension 2. Soit $W = \langle \binom{1}{1} \rangle$ le sous-espace de W engendré par le vecteur $\binom{1}{1}$.

   Donner une base de l'espace vectoriel quotient V/W. Démontrer votre réponse.

   (c) Démontrer le deuxième théorème d'isomorphisme pour les espaces vectoriels : Soient K un corps et V, W des K-espaces vectoriels. Alors, l'application

   $$\overline{\varphi} : V/(V \cap W) \to (V + W)/W, \quad v + (V \cap W) \mapsto v + W$$

   est un isomorphisme K-linéaire.

2. Soient A un anneau commutatif et $I, J, K \trianglelefteq A$ des idéaux. Démontrer :

   (a) $I \cap J$ est un idéal de A.

   (b) $I + J := \{i + j \mid i \in I, j \in J\}$ est un idéal de A.

   (c) $I \cdot J := \{\sum_{\ell=1}^{r} i_\ell j_\ell \mid r \in \mathbb{N}, i_\ell \in I, j_\ell \in J\}$ est un idéal de A.

   (d) $I + J = J + I$.

   (e) $(I \cdot J) \cdot K = I \cdot (J \cdot K)$.

   (f) $I \cdot (J + K) = I \cdot J + I \cdot K$.

3. Calculer l'ordre de tout élément du groupe $(\mathbb{Z}/12\mathbb{Z}, +, \overline{0})$.

À propos. La théorie des corps (commutatifs) se développe tout au long du XIXe siècle, en parallèle et de façon intimement liée avec la théorie des groupes, la théorie des anneaux et l'algèbre linéaire. Jusqu'à cette époque, l'algèbre s'identifie à la théorie des équations polynomiales et de leur résolution. C'est dans ce contexte qu'apparaissent les premières notions de théorie des corps, avec les travaux de Niels Abel et ceux d'Evariste Galois, même si la structure n'est pas identifiée explicitement.

Avec la naissance de l'étude des nombres algébriques, motivée par des problèmes de nature arithmétique, il est devenu nécessaire de préciser explicitement la structure de corps, en parallèle avec les notions d'entier algébrique, et d'anneau. C'est dans ce contexte que la structure de corps est introduite indépendamment (et de façons assez différentes) par Richard Dedekind et Leopold Kronecker. Le vocabulaire actuel vient de de Dedekind qui définit un corps (Körper en allemand, c'est la raison pour laquelle un corps quelconque est souvent nommé K) comme un sous-ensemble de nombres réels ou complexes stable par addition, soustraction, multiplication et division.

En 1893 Heinrich Weber donne la première véritable axiomatisation des corps (commutatifs), dans un article dont le but est de donner une présentation générale de la théorie de Galois. L'axiomatisation des théories mathématiques en est encore à ses balbutiements et Weber oublie (mais bien sûr utilise) l'associativité de la multiplication.

En 1910, Ernst Steinitz établit la théorie axiomatique des corps dans un mémoire fondateur de l'algèbre moderne.

Légèrement adapté de : `http ://fr.wikipedia.org/wiki/Corps_commutatif`

Exercices : Algèbre 2

Semestre d'été 2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David

Feuille 4

12/03/2013

Ces exercices sont à rendre le 19/03/2013 au début du cours. L'un/une d'entre vous présentera un des exercices lors du cours du 26/03/2013.

---

1. Dans cet exercice, vous allez démontrer le « théorème chinois ».
   (a) Pour s'échauffer... Soient $n = 11$ et $m = 15$.
      (1) Trouver $r, s \in \mathbb{Z}$ t.q. $1 = rn + ms$.
      (2) Utiliser (1) pour calculer $x, y \in \mathbb{Z}$ t.q.

$$x \equiv 0 \mod (n) \quad \text{et} \quad x \equiv 1 \mod (m)$$
$$y \equiv 1 \mod (n) \quad \text{et} \quad y \equiv 0 \mod (m)$$

      (3) Utiliser (2) pour calculer $z \in \mathbb{Z}$ t.q.

$$z \equiv 2 \mod (n) \quad \text{et} \quad z \equiv 7 \mod (m).$$

      Montrer ensuite que z peut être choisi t.q. $0 \leq z < nm = 165$ et que ce choix est unique.
   (b) Maintenant en général... Soient $n, m \in \mathbb{N}_{>1}$ avec $\mathrm{pgcd}(n, m) = 1$.
      (1) Montrer l'existence de $x, y \in \mathbb{Z}$ t.q.

$$x \equiv 0 \mod (n) \quad \text{et} \quad x \equiv 1 \mod (m)$$
$$y \equiv 1 \mod (n) \quad \text{et} \quad y \equiv 0 \mod (m)$$

      (2) Soient $a, b \in \mathbb{Z}$. Déduire de (1) l'existence de $z \in \mathbb{Z}$ t.q.

$$z \equiv a \mod (n) \quad \text{et} \quad z \equiv b \mod (m).$$

      Montrer ensuite que z peut être choisi t.q. $0 \leq z < nm$ et que ce choix est unique.
   (c) Maintenant la version abstraite...Soient encore $n, m \in \mathbb{N}_{>1}$ avec $\mathrm{pgcd}(n, m) = 1$. Démontrer que l'homomorphisme de groupes

$$\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, \quad a \mapsto (a + n\mathbb{Z}, a + m\mathbb{Z})$$

      est surjectif et que son noyau est égal à $nm\mathbb{Z}$. Puis, déduire du premier théorème d'isomorphisme que ϕ induit un isomorphisme $\overline{\phi} : \mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.
   (d) Finalement, décrire en une phrase pourquoi l'isomorphisme $\overline{\phi}$ de (c) est en effet une version abstraite de (b).

À propos. La forme originale du « théorème chinois », contenue dans un livre du mathématicien chinois Qin Jiushao publié en 1247, est un résultat concernant les systèmes de congruences. Selon Zachariou, le théorème des restes chinois aurait été découvert antérieurement par les Grecs. Mais on trouve trace d'un problème analogue dans le livre de Sun Zi, le Sunzi suanjing datant du IIIe siècle :

> Combien l'armée de Han Xing comporte-t-elle de soldats si, rangés par 3 colonnes, il reste deux soldats, rangés par 5 colonnes, il reste trois soldats et, rangés par 7 colonnes, il reste deux soldats ?

On peut penser que les Chinois, férus de calculs astronomiques, puissent être intéressés par des concordances de calendrier et qu'ils aient été amenés très tôt à s'intéresser à des questions du type :

> Dans combien de jours la pleine lune tombera-t-elle au solstice d'hiver ?

Si la question se pose alors qu'il reste 6 jours avant le solstice d'hiver et 3 jours avant la pleine lune, la question se traduit par :

> Existe-t-il un entier x tel que le reste de la division de x par 365 donne 6 et le reste de la division de x par 28 donne 3 ?

La résolution proposée par Sun Zi pour le problème des soldats est la suivante :

> Multiplie le reste de la division par 3, c'est-à-dire 2, par 70, ajoute lui le produit du reste de la division par 5, c'est-à-dire 3, avec 21 puis ajoute le produit du reste de la division par 7, c'est-à-dire 2 par 15. Tant que le nombre est plus grand que 105, retire 105.

Enfin, un problème concernant des pirates et un trésor, très fréquemment cité pour illustrer le théorème des restes chinois :

> Une bande de 17 pirates possède un trésor constitué de pièces d'or d'égale valeur. Ils projettent de se les partager également, et de donner le reste au cuisinier chinois. Celui-ci recevrait alors 3 pièces. Mais les pirates se querellent, et six d'entre eux sont tués. Un nouveau partage donnerait au cuisinier 4 pièces. Dans un naufrage ultérieur, seuls le trésor, six pirates et le cuisinier sont sauvés, et le partage donnerait alors 5 pièces d'or à ce dernier. Quelle est la fortune minimale que peut espérer le cuisinier s'il décide d'empoisonner le reste des pirates ?

Légèrement adapté de :
`http ://fr.wikipedia.org/wiki/Théorème_des_restes_chinois`

Exercices : Algèbre 2

Semestre d'été 2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David

Feuille 5

19/03/2013

Ces exercices sont à rendre le 26/03/2013 au début du cours. L'un/une d'entre vous présentera un des exercices lors du cours du 09/04/2013.

---

1. (a) Dans l'anneau $A = \mathbb{Z}/6\mathbb{Z}$, trouver deux diviseurs de zéro a et b dont la somme est une unité.
   (b) Dans l'anneau $A = \mathbb{Z}/6\mathbb{Z}$, trouver deux polynômes $f, g \in A[X]$ tels que
   $$\deg(f(X)g(X)) < \deg(f(X)) + \deg(g(X)).$$

2. Soit $f(X) = X^2 + 1 \in \mathbb{R}[X]$ et soit $\varphi : \mathbb{R}[X] \to \mathbb{C}$ l'unique homomorphisme d'anneaux tel que $\varphi(X) = i = \sqrt{-1}$ et $\varphi(x) = x$ pour $x \in \mathbb{R}$. Démontrer :
   (a) $f \in \ker(\varphi)$.
   (b) $f(X) = (X - i)(X + i)$.
   (c) Si $g \in \ker(\varphi) \subseteq \mathbb{R}[X]$, alors $g(-i) = 0$.
   Indication : Utiliser la conjugaison complexe.
   (d) Si $g \in \ker(\varphi)$, alors $f(X)$ divise $g(X)$.
   (e) $\ker(\varphi) = f(X)\mathbb{R}[X] = \{f(X)g(X) \mid g \in \mathbb{R}[X]\}$.
   (f) Le théorème d'isomorphisme donne un isomorphisme $\overline{\varphi} : \mathbb{R}[X]/(f(X)\mathbb{R}[X]) \to \mathbb{C}$.

À propos. Alice, une vieille dame qui a du mal à se déplacer, veut envoyer l'histoire de sa vie qu'elle a rédigée pendant deux ans, à son ami d'enfance Robert qui habite New York et qu'elle n'a pas vu depuis soixante ans. Comme elle ne peut pas aller à la poste elle-même, elle devrait confier son histoire à sa fille Gwendoline. Mais l'histoire de sa vie contient bien des passages que Gwendoline ne doit pas connaître. Connaissant sa fille, elle sait qu'elle ouvrirait la lettre dès qu'elle en aurait la possibilité. Elle réfléchit un peu et elle trouve une idée : Elle met l'histoire de sa vie dans une boîte et ferme la boîte avec un cadenas dont elle seule a la clé. Puis, elle demande à sa fille de porter la boîte à la poste et de l'expédier à Robert qui la reçoit une semaine après. Comme Robert n'a pas la clé du cadenas, il n'a pas accès à l'histoire d'Alice. Lui aussi il réfléchit... Deux semaines plus tard, il a lu l'histoire, et Gwendoline ne la connaît toujours pas.

Comment Alice et Robert ont-ils fait ?

Ceci est une version du *no key protocol* de Shamir.

Exercices : Algèbre 2

Semestre d'été 2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David

Feuille 6

26/03/2013

Ces exercices sont à rendre le 09/04/2013 au début du cours. L'un/une d'entre vous présentera un des exercices lors du cours du 16/04/2013.

---

1. Soient $f(X) = X^5 + 4X^4 + 4X^3 + 4X^2 + 4X + 3, g(X) = X^2 + 2X - 3 \in \mathbb{Q}[X]$. À l'aide de l'algorithme d'Euclide, calculez le pgcd (unitaire) $d(X)$ de $f(X)$ et $g(X)$ et représentez-le en combinaison $\mathbb{Q}[X]$-linéaire :
$$d(X) = a(X)f(X) + b(X)g(X).$$

2. Soit $b \in \mathbb{N}_{\geq 2}$ (la « base »). Pour $\ell \in \mathbb{N}$ et $a_0, a_1, \ldots, a_\ell \in \{0, 1, 2, \ldots, b-1\}$ nous considérons l'entier positif
$$n := \sum_{i=0}^{\ell} a_i b^i$$
que nous notons aussi $(a_\ell\, a_{\ell-1}\, \ldots\, a_1\, a_0)_b$. Nous disons que $(a_\ell\, a_{\ell-1}\, \ldots\, a_1\, a_0)_b$ est le *développement b-adique de n*.

   Exemple : Pour $b = 10$ nous avons $(327)_{10} = 327$. Pour $b = 2$ nous avons $(1101)_2 = 13$.

   (a) Quel nombre naturel est représenté par le développement 10-adique $(9821)_{10}$?

   (b) Quel nombre naturel est représenté par le développement 7-adique $(1361)_7$?

   (c) Quel nombre naturel est représenté par le développement 2-adique $(1100101)_2$?

   (d) Calculer le développement 7-adique de 199.

   (e) Calculer le développement 2-adique de 199.

   (f) Soit $b \in \mathbb{N}_{\geq 2}$. Démontrer que tout $n \in \mathbb{N}$ peut être écrit comme $n = (a_\ell\, a_{\ell-1}\, \ldots\, a_1\, a_0)_b$ avec des uniques $\ell \in \mathbb{N}$ et $a_0, a_1, \ldots, a_\ell \in \{0, 1, 2, \ldots, b-1\}$ tels que $a_\ell \neq 0$.
   Indication : Division euclidienne.

À propos. La première référence ayant influencé le monde mathématique sur la question de la division euclidienne est le livre VII, des Éléments d'Euclide datant d'environ 300 ans avant J.-C.. On y trouve la première définition théorique de la division et l'étude de ses conséquences. Cette branche des mathématiques prend le nom d'Arithmétique. Elle traite essentiellement des questions portant sur les nombres entiers.

Certains mathématiciens comme Diophante d'Alexandrie puis, bien plus tard, Pierre de Fermat comprennent la richesse de cette branche des mathématiques. Ils établissent quelques résultats comme le petit théorème de Fermat et formulent des conjectures comme le théorème des deux carrés de Fermat ou le grand théorème de Fermat. Un outil théorique important est l'analyse des propriétés du reste de la division euclidienne des membres d'une égalité d'entiers.

Cité de : `http ://fr.wikipedia.org/wiki/Anneau_euclidien`

Exercices : Algèbre 2

Semestre d'été 2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David

Feuille 7

09/04/2013

Ces exercices sont à rendre le 16/04/2013 au début du cours.

1. Trouver un générateur pour chacun des idéaux principaux suivants :
   (a) $(7, 3) \lhd \mathbb{Z}$,
   (b) $(7, -84) \lhd \mathbb{Z}$,
   (c) $(11) \cap (91, 39) \lhd \mathbb{Z}$,
   (d) $(X^3 + 17X^2 + 29X, X^2 + 2X) \lhd \mathbb{Q}[X]$.
2. Démontrer que l'idéal $(2, X)$ de $\mathbb{Z}[X]$ (c'est-à-dire, l'idéal de $\mathbb{Z}[X]$ engendré par 2 et X) n'est pas un idéal principal.
3. Notons $i = \sqrt{-1} \in \mathbb{C}$. Soit $\mathbb{Z}[i]$ l'ensemble $\{a + ib \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$, appelé les *entiers de Gauß*.
   (a) Démontrer que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$.
   (b) Soit $\delta : \mathbb{Z}[i] \to \mathbb{C}$ l'application donnée par $a + bi \mapsto a^2 + b^2 = (a + ib)(a - ib) = |a + ib|^2$. Démontrer que $\mathbb{Z}[i]$ est un anneau euclidien pour la fonction δ.
   Indication : Pour obtenir la division euclidienne de $a + bi$ par $c + id \neq 0$, choisissez $e + if \in \mathbb{Z}[i]$ « près » du quotient $\frac{a+ib}{c+id} \in \mathbb{C}$.

À propos. Les entiers de Gauß ont été découverts alors que Gauß recherche une solution à la question des congruences des carrés étudiée dans un premier temps par Fermat. Euler formalise la notion de résidu quadratique et conjecture la solution, c'est-à-dire la loi de réciprocité quadratique. Legendre reprend le théorème et propose une preuve incomplète et insuffisante.

À l'âge de 18 ans, Gauß démontre le théorème. La démonstration est publiée trois ans plus tard. Il considère cette loi comme le joyau de l'arithmétique, l'appelant même le « théorème d'or ». Pour résoudre cette question, il découvre un ensemble : celui des entiers qui portent maintenant son nom. Ils bénéficient des mêmes propriétés arithmétiques que les entiers relatifs. On y trouve la division euclidienne, l'équivalent du lemme d'Euclide, de l'identité de Bézout, des nombres premiers et du théorème fondamental de l'arithmétique. À l'aide de cette structure, il redémontre le théorème des deux carrés conjecturé par Fermat et démontré par Euler et ouvre la voie de l'arithmétique modulaire.

L'étude de ce type de structure est alors largement développée par des mathématiciens comme Dedekind ou Hilbert et prend le nom de théorie des anneaux.

Adapté de : `http ://fr.wikipedia.org/wiki/Entier_de_Gauss`

Exercices : Algèbre 2

Semestre d'été 2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David

Feuille 8

16/04/2013

Ces exercices qui ne sont pas à rendre vous préparent au devoir surveillé du 23/04/2013.

---

1. Soit $b \in \mathbb{N}_{\geq 2}$ (la « base »). Pour $\ell \in \mathbb{N}$ et $a_0, a_1, \ldots, a_\ell \in \{0, 1, 2, \ldots, b-1\}$ nous considérons l'entier positif

$$n := \sum_{i=0}^{\ell} a_i b^i$$

que nous notons aussi $(a_\ell\, a_{\ell-1}\, \ldots\, a_1\, a_0)_b$. Nous disons que $(a_\ell\, a_{\ell-1}\, \ldots\, a_1\, a_0)_b$ est le *développement b-adique de n*.

   (a) Quel nombre naturel est représenté par le développement 2-adique $(10010111)_2$?

   (b) Calculer le développement 2-adique de 361.

2. Soient $f(X) = X^6 + 4X^2 + 7X + 3, g(X) = X^2 + X - 3 \in \mathbb{Q}[X]$. À l'aide de l'algorithme d'Euclide, calculez le pgcd (unitaire) $d(X)$ de $f(X)$ et $g(X)$ et représentez-le en combinaison $\mathbb{Q}[X]$-linéaire :

$$d(X) = a(X)f(X) + b(X)g(X).$$

3. (a) Soit K un corps. Combien d'idéaux possède K ? Dresser la liste complète des idéaux de K.

   (b) Soient K un corps, A un anneau différent de $\{0\}$ et $\varphi : K \to A$ un homomorphisme d'anneaux. Démontrer : φ est injectif.

4. Soit A un anneau commutatif. Un élément $x \in A$ est appelé *nilpotent* s'il existe $n \in \mathbb{N}$ t.q. $x^n = 0$. Démontrer :

   (a) Si $x \in A$ est nilpotent, alors $1 + x$ est une unité dans A.
   Indication : Somme géométrique.

   (b) Si $x \in A$ est nilpotent et $a \in A^\times$ est une unité, alors $a + x$ est aussi une unité dans A.
   Indication : Utiliser (a).

   (c) (Exercice supplémentaire) Soit $f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in A[X]$ un polynôme. Alors :

$$f(X) \text{ est une unité dans } A[X] \Leftrightarrow a_0 \in A^\times \text{ et } a_1, \ldots, a_n \text{ sont nilpotents dans } A.$$

   Indication : $\Leftarrow$: Utiliser (b). $\Rightarrow$: Par récurrence (pour $n \geq 1$) : Si $b_m X^m + \cdots + b_0$ est l'inverse de $f(X)$, montrer par récurrence (sur r) que $a_n^{r+1} b_{m-r} = 0$ et en déduire que a_n est nilpotent ; ensuite, utiliser (b) pour réduire le degré.

Exercices : Algèbre 2

Semestre d'été 2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David

Feuille 9

23/04/2013

Ces exercices sont à rendre le 30/04/2013 au début du cours. L'un/une d'entre vous présentera un des exercices lors du cours du 07/05/2013.

---

1. Soit $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ le corps à deux éléments. On considère le polynôme $f(X) = X^2 + X + 1 \in \mathbb{F}_2[X]$.
   (a) Démontrez que $f(X)$ est un élément irréductible de $\mathbb{F}_2[X]$.
   (b) Soit $R := \mathbb{F}_2[X]/(f(X))$. Faites une liste des éléments de R (il y en a 4).
   (c) Nous savons que R est un anneau commutatif. Écrivez la table d'addition et la table de multiplication de R. Déduisez que R est un corps à 4 éléments.
   (d) (Exercice supplémentaire) Trouvez un corps à 16 éléments et un corps à 27 éléments. (N'écrivez pas les tables d'addition et de multiplication !)
2. Nous savons que $\mathbb{Z}[i] = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ est un anneau euclidien, donc un anneau principal. On a l'égalité $2 = (1 + i)(1 - i)$. Démontrer :
   (a) $1 + i$ et $1 - i$ sont associés dans $\mathbb{Z}[i]$.
   (b) $1 + i$ est irréductible dans $\mathbb{Z}[i]$ (donc premier par la proposition 6.6 du cours).

   Ces calculs ont donné la factorisation de 2 en éléments premiers dans $\mathbb{Z}[i]$.
3. Considérons l'anneau $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$. On a l'égalité
$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$
   (a) Démontrer que 1 et -1 sont les seules unités dans $\mathbb{Z}[\sqrt{-5}]$.
   (b) Déduire que $1 + \sqrt{5}$, $1 - \sqrt{-5}$, 2 et 3 ne sont pas associés deux à deux dans $\mathbb{Z}[\sqrt{-5}]$.
   (c) Démontrer que $1 + \sqrt{5}$, $1 - \sqrt{-5}$, 2 et 3 sont irréductibles dans $\mathbb{Z}[\sqrt{-5}]$.

   Ces calculs montrent que 6 ne s'écrit pas de façon unique comme produit d'éléments irréductibles (donc, dans la terminologie à introduire dans le cours, $\mathbb{Z}[\sqrt{-5}]$ n'est pas un anneau factoriel).

À propos. Pour le loisir mathématiques : des BD gratuites sur :
`http://www.savoir-sans-frontieres.com`

Exercices : Algèbre 2

Semestre d'été 2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David

Feuille 10

30/04/2013

Ces exercices sont à rendre le 07/05/2013 au début du cours. L'un/une d'entre vous présentera un des exercices lors du cours du 14/05/2013.

---

1. Soient A un anneau et $I \trianglelefteq A$ un idéal. Démontrer : S'il existe une unité $u \in A^\times$ telle que $u \in I$, alors $I = A$.
2. Dans cet exercice vous allez construire le *corps des fractions* d'un anneau intègre A. La construction est une généralisation directe de la construction des nombres rationnels $\mathbb{Q}$ à partir des entiers relatifs $\mathbb{Z}$ (voir Algèbre 1, 6.1 et 6.2).

   Soit A un anneau intègre. Sur $A \times (A \setminus \{0\})$ on définit une relation

   $$(a, x) \sim (b, y) \Leftrightarrow ay = bx.$$

   (a) Démontrer : C'est une relation d'équivalence et la classe de (a, x) est formée de tous les (b, y) tels que $ay = bx$.

   On utilisera la notation $\frac{a}{x}$ pour la classe $\overline{(a, x)}$. L'ensemble quotient est noté $\mathrm{Frac}(A)$. Pour la suite on pose $K := \mathrm{Frac}(A)$.

   (b) Démontrer : Les deux applications

   $$+ : K \times K \to K, \quad \frac{a}{x} + \frac{b}{y} := \frac{ay + bx}{xy}$$

   et

   $$\cdot : K \times K \to K, \quad \frac{a}{x} \cdot \frac{b}{y} := \frac{ab}{xy}$$

   sont bien définies, c'est-à-dire que leurs définitions ne dépendent pas des choix des représentants (a, x) et (b, y) des classes $\frac{a}{x}$ et $\frac{b}{y}$.

   (c) Démontrer : $(K, +, \cdot, \frac{0}{1}, \frac{1}{1})$ est un corps, c'est le *corps des fractions* de A.

   (d) Démontrer : L'application

   $$\iota : A \to K, \quad a \mapsto \frac{a}{1}$$

   est injective et on a $\iota(a + b) = \iota(a) + \iota(b)$ et $\iota(a \cdot b) = \iota(a) \cdot \iota(b)$ pour tous $a, b \in K$.

À propos. Dix mathématiciens honnêtes et sincères sont assis l'un derrière l'autre de façon à ce que le premier ne voie personne d'autre, le deuxième ne voie que le premier, le troisième ne voie que le premier et le deuxième, etc. On leur met des chapeaux rouges ou jaunes. Personne ne voit la couleur de son chapeau. Dès qu'un des mathématiciens connaît la couleur de son chapeau, il doit la dire. On leur donne l'information qu'il y a au moins un chapeau de chaque couleur.

Est-ce que le premier mathématicien connaîtra la couleur de son chapeau ?

Exercices : Algèbre 2

Semestre d'été 2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David

Feuille 11

07/05/2013

Ces exercices sont à rendre le 14/05/2013 au début du cours. L'un/une d'entre vous présentera un des exercices lors du cours du 21/05/2013.

---

1. (a) Soient K un corps et $f \in K[X]$ un polynôme de degré 2 ou 3. Démontrer l'équivalence : f est irréductible $\Leftrightarrow f(a) \neq 0$ pour tout $a \in K$.
   (b) Dresser la liste complète de tous les polynômes irréductibles de $\mathbb{F}_2[X]$ de degré $1, 2, 3$.
   (c) Donner un exemple qui montre que l'équivalence dans (a) n'est pas vraie pour les polynômes de degré ≥ 4.
   (d) Nous savons que $\mathbb{F}_2[X]$ est un anneau factoriel. Calculer la factorisation en polynômes irréductibles de $X^8 + X^7 + X + 1 \in \mathbb{F}_2[X]$.
2. Cet exercice utilise le corps des fractions introduit sur la feuille 10.
   (a) Soit K un corps commutatif. On pose $A := K[X]$ (on sait que c'est un anneau intègre) et $K(X) := \mathrm{Frac}(K[X])$; $K(X)$ est appelé le *corps des fractions rationnelles* (à une indéterminée). Démontrer que toute classe d'équivalence $\overline{(f(X), g(X))}$ dans $K(X)$ a un unique représentant $(a(X), b(X))$ avec $\mathrm{pgcd}(a(X), b(X)) = 1$ et $b(X) \neq 0$ unitaire.
   Calculer ce représentant dans l'exemple $\overline{(X^2 + 2X + 1, 1 - X^2)} = \frac{X^2+2X+1}{1-X^2} \in \mathbb{Q}(X)$.
   (b) Soient K un corps et $A \subseteq K$ un sous-anneau. Démontrer que A est un anneau intègre et que le corps des fractions de A est contenu dans K.
   Indication : écrire un homomorphisme naturel $\mathrm{Frac}(A) \to K$.
   (c) Trouver un anneau A t.q. $\mathbb{Z} \subsetneq A \subsetneq \mathbb{Q}$ et déterminer $\mathrm{Frac}(A)$.

À propos. Une illustration de l'Axiome du choix due à Bertrand Russell

Bertrand Russell disait à propos de l'axiome du choix : Pour choisir une chaussette plutôt que l'autre pour chaque paire d'une collection infinie, on a besoin de l'axiome du choix. Mais pour les chaussures, ce n'est pas la peine.

Explication :

- Quand on dispose d'une paire de chaussettes quelconque, on n'a aucun moyen a priori de distinguer une chaussette de l'autre, ce sont des objets a priori identiques et même si chaque matin on arrive à choisir celle qu'on va mettre en premier, on serait bien en peine de trouver un procédé général qui nous permette de renouveler l'exploit éternellement.
- Pour les chaussures, il existe un moyen de choisir qui marche tout le temps (une fonction de choix naturelle) : choisir toujours la chaussure gauche (ou droite) puisqu'il y a toujours une chaussure gauche et une chaussure droite.

Cité de : `http://fr.wikipedia.org/wiki/Axiome_du_choix`

Exercices : Algèbre 2

Semestre d'été 2013

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Agnès David

Feuille 12

14/05/2013

Ces exercices sont à rendre le 21/05/2013 au début du cours. L'un/une d'entre vous présentera un des exercices lors du cours du 28/05/2013.

---

1. Soit A un anneau. Démontrer :
   A est intègre $\Leftrightarrow$ (0) est un idéal premier.
2. Lesquels des idéaux suivants sont premiers, lesquels sont maximaux ? Démontrer les réponses.
   (a) $(3) \lhd \mathbb{Z}$
   (b) $(7) \cap (11) \lhd \mathbb{Z}$
   (c) $(289, 255) \lhd \mathbb{Z}$
   (d) $(X^2 + 1) \lhd \mathbb{Q}[X]$
   (e) $(X^2 + 1) \lhd \mathbb{C}[X]$
   (f) $(X^2 + 1) \lhd \mathbb{F}_5[X]$
   (g) $(X^2 + 1) \lhd \mathbb{F}_7[X]$
   (h) $(0) \lhd \mathbb{Z}/57\mathbb{Z}$
   (i) $(0) \lhd \mathbb{Z}/53\mathbb{Z}$
   (j) $(X^3 - 1, X^2 + X + 1) \lhd \mathbb{Q}[X]$
   (k) $(X^2 + X + 1, 2) \lhd \mathbb{Z}[X]$.
3. (a) Soient p un nombre premier et $f(X) = \sum_{i=0}^{d} a_i X^i \in \mathbb{Z}[X]$ un polynôme unitaire de degré d. Soit $I = (p, f(X))$ l'idéal de $\mathbb{Z}[X]$ engendré par p et $f(X)$.
   On note $\overline{f}(X) = \sum_{i=0}^{d} \overline{a_i} X^i \in \mathbb{F}_p[X]$ la réduction de f modulo p (où $\overline{a_i}$ est la classe de a_i modulo p). En utilisant l'application « réduction des coefficients modulo p » $\mathbb{Z}[X] \twoheadrightarrow \mathbb{F}_p[X]$ suivie par l'application « projection » $\mathbb{F}_p[X] \twoheadrightarrow \mathbb{F}_p[X]/(\overline{f}(X))$ et le premier théorème d'isomorphisme, démontrer que $\mathbb{Z}[X]/I$ est isomorphe à $\mathbb{F}_p[X]/(\overline{f}(X))$.
   (b) On suppose de plus que $\overline{f}(X)$ est un élément irréductible de $\mathbb{F}_p[X]$. Déduisez de (a) que l'idéal $I = (p, f(X)) \lhd \mathbb{Z}[X]$ est un idéal maximal.
   (c) (Exercice supplémentaire) Soit $I \lhd \mathbb{Z}[X]$ un idéal maximal. Démontrer qu'il existe un nombre premier p et un polynôme unitaire $f(X) \in \mathbb{Z}[X]$ t.q. $I = (p, f(X))$ et $\overline{f}(X)$ est un élément irréductible de $\mathbb{F}_p[X]$.
   Indication : Démontrer d'abord que le corps $\mathbb{Z}[X]/I$ est de caractéristique $p > 0$. Déduire que I contient le nombre premier p. Utiliser ensuite que le corps $\mathbb{Z}[X]/I$ est isomorphe à $\mathbb{F}_p[X]/(\overline{f}(X))$ pour un certain polynôme irréductible $\overline{f}(X) \in \mathbb{F}_p[X]$, car $\mathbb{F}_p[X]$ est un anneau principal. Finalement, démontrer que $I = (p, f(X))$ où $f(X)$ est n'importe quel polynôme unitaire dans $\mathbb{Z}[X]$ dont la réduction modulo p est $\overline{f}(X)$.

À propos. D'après mon expérience, les démonstrations où entrent en jeu des matrices peuvent être abrégées de moitié si l'on expulse les matrices.

(Emil Artin, Algèbre géométrique, Chapitre 1)