Défense de Plan

La notion d'anneaux principal est une structure algébrique centrale en mathématiques. Une première manière de l'appréhender peut être de la voir comme une généralisation de l'anneau de entiers relatifs. Comprendre l'intérêt l'intérêt d'une telle structure peut être utile vu qu'on utilise quotidiennement les nombres.
Le plan proposé se découpe en deux parties.

Une première assez théorique qui essaye de dégager les poser certaines notions primordiales comme la notion d'anneau factoriel, d'anneau euclidien. Leur lien avec la notion d'anneau prinicipal.
Tout cela est fait dans le but de pratiquer aisément l'arithmétique sur de tels ensembles. On souhaite ou a souhaité comprendre en profondeur ce que l'on faisait sur $\mathbb{Z}$ qui d'ailleurs est principal !
On aborde aussi le lien entre la théorie des corps et la théorie des anneaux principaux principalement au travers de l'anneau des polynômes correspondant à un anneau donné.

La deuxième partie est là pour montrer des applications de la notion présentée. J'ai choisi, premièrement, de proposer une présentation de l'algorithme découvert par Berlekamp au milieu des années 60. Il a proposé un algorithme pour écrire un polynôme sous forme de produit d'irréductible.
Elle se place sur des corps finis. Les corps finis étant des anneaux principaux. C'est donc une application qui trouve toute sa place dans l'algèbre linéaire et le calcul formel. Elle des intérêts bien évident en informatique pour la rapidité de calcul par exemple.
Le deuxième développement est une démonstration du théorème des deux carrés de Fermat qui exprime une caractérisation des entiers de la forme $n = a^2 + b^2$. La démonstration présentée est du à Richard Dedekind. Elle utilise le fait que l'anneau des entiers de Gauss $\mathbb{Z}[i]$ est euclidien et quelques propriétés autour des nombres premiers et de cet anneau.

I Leçon 122 : Anneaux Principaux. Applications.

Dans tout le plan on suppose que A est un anneau commutatif et intègre.

a Arithmétique et Anneaux Principaux

a.1 Notions d'Arithmétique

Définition 1. On note $A^* = \{a \in A \backslash \exists b \in A, ab = 1\}$ ensemble des inversibles de A.

Remarque 1. On a $a \in A^* \Leftrightarrow (a) = A$

Exemple 1.
- Les inversibles de $\mathbb{Z}$ sont -1 et 1.
- Les inversibles d'un corps quelconques sont tout les élements non nuls.

Définition 2. Soient $a, b \in A$, on dit que b divise a s'il existe $k \in A$ tq b=ak.

Proposition 1. b divise a si et seulement si $(a) \subset (b)$

Définition 3. On définit la relation d'équivalence **R** par $a\mathbf{R}b \Leftrightarrow (a) = (b) \Leftrightarrow$ b divise a et a divise b.
On dit que a et b sont associés

Proposition 2. $a\mathbf{R}b \Leftrightarrow \exists u \in A^*$ tel que a=bu

Définition 4. Soit $p \in A$, p est irréductible si et seulement si p n'est pas inversible et si p=ab alors a ou b est inversible.

Exemple 2.
- 0 n'est pas irréductible.
- Les irréductibles de $\mathbb{Z}$ sont les nombres premiers.

Définition 5. Soit $a, b \in A$, a et b sont premiers entre eux (ou étrangers) si $\forall d \in A$, d divise a et d divise b alors d est inversible.

a.2 Idéaux et Anneaux Principaux

Définition 6. Soit I un idéal de A. I est premier si $A \neq I$ et $\forall a, b \in A$, si $ab \in I$ alors $a \in I$ ou $b \in I$

Définition 7. Soit I un idéal de A. I est principal si $\exists a \in I$ tel que $I = (a)$.

Exemple 3. Tout les idéaux de $\mathbb{Z}$ sont principaux.

Définition 8. Un anneau est principal si tout idéal est principal.

Exemple 4.
- $\mathbb{Z}$ est principal
- Tout les corps sont des anneaux principaux.

Définition 9. A est factoriel si :

- A est intègre
- $\forall a \in A^*$, $a = up_1 \dots p_r$, avec u inversible et les $p_1 \dots p_r$ irréductibles.
- Cette décomposition est unique à permutation près et à des inversibles près.

Exemple 5.
- $\mathbb{Z}$ est factoriel.
- $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel car $2*3 = (1+i\sqrt{5})(1-i\sqrt{5})$ et tout les facteurs en jeu sont irréductibles.

Proposition 3. On suppose que A vérifie le deuxième item de la définition précendente alors : A vérifie le troisième item :

- si et seulement si A vérifie le lemme d'euclide : si p irréductible et p divisant ab alors p divise a ou p divise b.
- si et seulement si p irréductible $\Leftrightarrow$ (p) est premier
- si et seulement si A vérifie le théorème de Gauss : si a divise bc et a est premier avec b alors a divise c.

Théorème 1. Un anneau principal est factoriel.

Définition 10. Soit A principal, et $a, b \in A$. On pose :

- (a)+(b)=(d), on dit que d est un pdcd de a et b
- (a)$\cap$(b)=(m), on dit que m est un ppcm de a et b

Proposition 4. Les élements d et m définit ci dessus correspondent aux pgcd et ppcm définit dans les anneaux factoriels.

a.3 Le cas des anneaux euclidiens

Définition 11. A est dit muni d'une stathme s'il existe $v : A\backslash\{0\} \longrightarrow \mathbb{N}$ tel que si $a, b \in A\backslash\{0\}$, $\exists (q, r) \in A^2$ tel que a=bq+r avec r=0 ou $v(r) \leq v(b)$.
Si V existe et A intègre alors A est euclien.

Exemple 6.
- $\mathbb{Z}$ est eucidien avec la norme absolue restreinte à $\mathbb{Z}$

Contre-Exemple 1. $\mathbb{Z}/3\mathbb{Z}$ est muni d'un stathme (la division euclidienne) mais n'est pas euclidien car il n'est pas intègre.

Théorème 2. Un anneau euclidien est principal.

Théorème des restes chinois

Théorème 3. (Une version du théorème des restes chinois)
Soient $m, n \in \mathbb{N}$, alors $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ si et seulement si m et n sont premiers entre eux.

Application 1. si $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ alors card($\mathbb{Z}/n\mathbb{Z}$)= $n \prod_{i=1}^{r} (1 - \frac{1}{p_i})$

Reconnaitre un anneau non euclidien

Proposition 5. A euclidien, il existe $x \in A$ tel que la restriction à $A^* \cup \{0\}$ de la projection canonique de A sur $A/\{x\}$ soit surjective.

Proposition 6. $\mathbb{Z}/n\mathbb{Z}$ possède un stathme.

Application 2. $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ n'est pas euclidien.

a.4 Passage à l'anneau des polynômes

Théorème 4. (Théorème de Gauss) Si A est factoriel alors A[X] est factoriel

Exemple 7.
- De ce fait $\mathbb{Z}[X]$ est factoriel.

Proposition 7. A[X] est principal si et seulement si A est un corps.

Lemme 1. (Division Euclidienne)
Soit $P \in$A[X], $P \neq 0$ et son coefficient dominant est inversible. Soit $F \in$A[X], il existe $Q, R \in$A[X] tel que F=PQ+R avec R=0 ou $degR \leq degP$

Proposition 8. Si K est un corps alors K[X] est euclidien.

Corollaire 1. A[X] principal $\Leftrightarrow$ A[X] euclidien $\Leftrightarrow$ A corps

Exemple 8. Dans $\mathbb{Z}[X]$, l'idéal engendré par X et 2 n'est pas principal donc $\mathbb{Z}[X]$ n'est pas principal.

Proposition 9. Soit $P \in A[X]$ avec $degP \geq 1$, irréductible dans K[X] où K est son corps de fraction et le pgcd des coefficient de P est égal à 1

b Applications

b.1 Eléments Algébriques

Définition 12. Soient K et L des corps avec $K \subset L$. L extension de K.

Exemple 9.
- $\mathbb{C}$ est une extension de $\mathbb{R}$.

Définition 13. Soit $K \subset L$ une extension et soient $\alpha \in L$ et $\varphi : K[X] \longrightarrow L$ tel que $\varphi(X) = \alpha$ et $\varphi_{|K} = id_K$.
Si φ n'est pas injectif on dit que α est algébrique sur K. i.e il existe $P \in K$ tel que P(α)=0.
Par définition, P est le polynôme minimal de α.

Exemple 10. $\sqrt{2}$, i sont algébrique sur $\mathbb{Q}$

Définition 14. $K \subset L$ algébrique si $\forall x \in L$, x est algébrique sur K.

b.2 Algèbre Linéaire et Calcul Formel

Pour cette partie, $\mathbb{K}$ est un corps, E est un $\mathbb{K}$-espace vectoriel de dimenson finie n et $f \in \mathbf{L}(E)$.

Lemme 2. (Lemme des Noyaux)
Soit $P \in$ K[X], tel que $P = \prod_{i=1}^{r} P_i^{\alpha_i}$ avec les P_i irréductibles et distincts deux à deux et $P(f) = 0$.
Alors $E = Ker(P_1^{\alpha_1}(f)) \oplus \cdots \oplus Ker(P_1^{\alpha_1}(f))$

Définition 15. $I = \{P \in K[X] \text{ tel que } P(f) = 0\} \neq \{0\}$ est l'idéal annulateur de f. On note π_f le polynôme unitaire tel que (π_f)=I.

Corollaire 2. Tout endomorphisme est diagonalisable par blocs.

Proposition 10. f est diagonalisable si et seulement si son polynôme minimal est scindé à racines simples sur K.

Théorème 5. (Algorithme de Berlekamp)(Développement 1)
Soient $q = p^n$ avec p premier et $n \in \mathbb{N}^*$ et $P \in \mathbb{F}_q[X]$ qui est sans facteur carré.
On pose $P = \prod_{i=1}^{r} P_i$, la décomoosition en produit d'irréductible sur $\mathbb{F}_q[X]$.
Si $r = 1$, alors P est irréductible sinon il existe $a \in \mathbb{F}_q$ et $V \in \mathbb{F}_q[X]$ tel que $pgcd(P, V - \alpha)$ soit un facteur non trivial de P.

b.3 Un exemple en théorie des nombres

Définition 16. On définit l'anneau des entiers de Gauss par $\mathbb{Z}[i] = \{a+ib \backslash a, b \in \mathbb{Z}\}$. Cet anneau est muni de $N : z = a + ib \in \mathbb{Z}[i] \longmapsto a^2 + b^2$ appellé norme.
Elle est multiplicative : $\forall x, y \in \mathbb{Z}[i]$, N(xy)=N(x)N(y).

Proposition 11. (Développement 2)
Les inversible de $\mathbb{Z}[i]$ sont $\{-1, -i, 1, i\}$.

Proposition 12. (Développement 2)
$\mathbb{Z}[i]$ est euclidien

Définition 17. On pose σ=$\{n \in \mathbb{Z}/a, b \in \mathbb{Z} \text{ tel que } n = a^2 + b^2\}$

Remarque 2. On remarque que $n \in \sigma \Leftrightarrow \exists z \in \mathbb{Z}[i]$, tel que N(z)=n.

Proposition 13. Soit p un nombre premier différent de 2.
Alors $x \in \mathbb{F}_p$ est un carré si et seulement si $x^{\frac{p-1}{2}} = 1$.

Corollaire 3. -1 est un carré dans $\mathbb{F}_p$ si et seulement si p=1 mod 4 ou p=2.

Lemme 3. (Développement 2)
σ est stable par multiplication.

Lemme 4. (Développement 2)
Si p est premier tel que p = 3 mod 4 alors $p \notin \sigma$.

Lemme 5. (Développement 2)
Soit p premier. Alors $p \in \sigma$ si et seulement si p n'est pas irréductible dans $\mathbb{Z}[i]$.

Définition 18. Soit p un nombre premier, on définit $v_p(n)$ la valuation p-adique définie comme le plus grand entier k tel que p^k divise n.

Remarque 3. On peut ainsi écrire pour tout entier n que $n = \prod_{p \in \mathbf{P}} p^{v_p(n)}$ où $\mathbf{P}$ est l'ensemble des nombres premiers.

Théorème 6. (Théorème des deux carrés de Fermat)(Développement 2)
Soit n un entier non nul. Alors $n \in \sigma$ si et seulement si $v_p(n)$ est pair pour tout p premier tel que p=3 mod 4.

c Développement

d Algorithme de Berlekamp

On rappelle le théorème des restes chinois qui nous sera utile dans la démonstration :

Théorème 7. Soient $P_1, \dots, P_r \in \mathbb{F}_q[X]$ polynômes premiers entre eux deux à deux. On pose $P = \prod_{i=1}^{r} P_i$. Alors
$$\begin{array}{ccc} \mathbb{F}_q/(P) & \longrightarrow & \mathbb{F}_q/(P_1) \times \cdots \times \mathbb{F}_q/(P_r) \\ x(modP) & \longmapsto & (x(modP_1), \dots, x(modP_r)) \end{array}$$

On énonce l'algorithme de Berlekamp :

Théorème 8. Soient $q = p^n$ avec p premier et $n \in \mathbb{N}^*$ et $P \in \mathbb{F}_q[X]$ qui est sans facteur carré. On pose $P = \prod_{i=1}^{r} P_i$, la décomoosition en produit d'irréductible sur $\mathbb{F}_q[X]$.
Si $r = 1$, alors P est irréductible sinon il existe $a \in \mathbb{F}_q$ et $V \in \mathbb{F}_q[X]$ tel que $pgcd(P, V - \alpha)$ soit un facteur non trivial de P.

Preuve. Considérons T : $\begin{array}{ccc} \mathbb{F}_q[X] & \longrightarrow & \mathbb{F}_q[X]/(P) \\ Q & \longmapsto & Q^q(modP) \end{array}$ Comme $S : Q \longmapsto Q^q$ et la projection canonique sont deux applications $\mathbb{F}_q$-linéaires on peut conclure que T est $\mathbb{F}_q$-linéaire par composition.
$\forall Q \in \mathbb{F}_q[X]$, $T(QP) = (QP)^q[P] = 0$ donc $(P) \subset Ker(T)$.
On peut alors factoriser T pour obtenir un $\mathbb{F}_q$-endormorphisme φ de $\mathbb{F}_q[X]/(P)$ défini par $\varphi([Q]) = [Q^q]$ en notant [Q] la classe d'équivalence de Q.
Les (P_i) sont premiers entre eux donc d'après le théorème des restes chinois, il existe $\Psi : \mathbb{F}_q/(P) \longrightarrow \mathbb{F}_q/(P_1) \times \cdots \times \mathbb{F}_q/(P_r)$
Et pour tout $1 \leq i \leq r$, $F_q/(P_i)$ est un corps car P_i est irréductible.
On pose $f = \Psi \circ \varphi \circ \Psi^{-1}$ application linéaire vérifiant $\forall Q = (Q_1, \dots, Q_r) \in \mathbb{F}_q/(P_1) \times \cdots \times \mathbb{F}_q/(P_r)$, $f(Q) = (Q_1^q, \dots, Q_r^q)$ car Ψ préserve la multiplication.
Donc on a pour $Q \in Ker(f - I_d) \Leftrightarrow Q_i^q = Q_i$ pour tout $1 \leq i \leq r$.
Or pour tout $1 \leq i \leq r$, $\mathbb{F}_q/(P_i)$ est une extension de $\mathbb{F}_q$ donc on a $Q_i^q = Q_i$
$\Leftrightarrow Q_i \in \mathbb{F}_q$.
Donc card(Ker$(f - I_d)$=q^r donc
dim(Ker$(\varphi - I_d)$)=dim(Ker(f-I_d))=r.

Supposons maintenant que $r \geq 2$, les polynômes constants modulo P forment un sous espace vectioriel de $\mathbb{F}_q/(P)$ de dimension 1 et il est engendré par 1.
De plus dim(Ker$(\varphi - I_d)$=$r \geq 2$, il $V \in *\mathbb{F}_q[X]$ non constant modulo P tel que $V^q = V$ (mod P).
En particulier, pour tout $1 \leq i \leq r$, on a V^q= V (mod P_i).
On pose $\alpha_i = V(modP_i) \in \mathbb{F}_q$.
Si pour tout $1 \leq i, j \leq r$, $\alpha_i = \alpha_j$ alors il existe $\alpha \in \mathbb{F}_q$ tel que $V = \alpha$ (mod P_i) pour tout $1 \leq i \leq r$.
grâce à l'injectivité de Ψ, $V = \alpha$ (mod P) est impossible car on a supposé n'est pas constant modulo P.

Donc il existe deux indices i et j tel que $\alpha_i \neq \alpha_j$.
On pose alors Q=pgcd(P,V-α_i). Mais P_i divise P et (V-α_i) donc il divise aussi Q.
De plus, P_j ne divise pas Q car il ne divise pas V-α_i puisque $\alpha_i \neq \alpha_j$.
Donc $Q \neq 1$, $Q \neq P$ et Q est un facteur non trivial de P.

Remarque 4.
- C'est une preuve constructive qui fournit un algorithme de calcul. Ici il suffit de calculer le noyau de l'application linéaire $\varphi - I_d$.
  Il est itératif, il faut recommencer avec $P/(V - \alpha)$ et il s'arrête quand dim(Ker($\varphi - I_d$)=1. Ce qui équivaut à la situation où le polynôme est irréductible.
-

e Théorèmes des deux carrés de Fermat

e.1 Quelques lemmes préliminaires

Proposition 14. Les inversible de $\mathbb{Z}[i]$ sont $\{-1, -i, 1, i\}$.

Preuve. Soit z inversible, $N(zz^{-1}) = N(z)N(z^{-1}) = N(1) = 1$. Donc N(z)=1 ou N(z) = -1.
Mais N est à valeurs dans $\mathbb{N}$ donc N(z)=1.
Soit z=a+ib tel que N(z)=1 $\Leftrightarrow a^2 + b^2 = 1$ donc soit a=0 soit b=0.
Donc $z \in \{-1, -i, 1, i\}$.

Proposition 15. $\mathbb{Z}[i]$ est euclidien

Preuve. N jouera le rôle de stathme euclidien de $\mathbb{Z}[i]$.
Soit $z, t \in \mathbb{Z}[i]$ tel que $t \neq 0$. On cherche $q, r \in \mathbb{Z}[i]$ tel que z=qt+r et $N(r) \leq N(t)$.
On pose $\frac{z}{t} = x + iy \in \mathbb{C}$ avec $x, y \in \mathbb{R}$ et q=a+ib avec $a, b \in \mathbb{N}$ tel que :
$|x - a| \leq \frac{1}{2}$ et $|y - b| \leq \frac{1}{2}$.
Alors $|\frac{z}{t} - q|^2 = (x - a)^2 + (y - b)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$.
On pose r=z-qt mais N(r)=$|r|^2 = |t|^2|\frac{z}{t} - q|^2 < |t|^2$=N(t).
Donc N est bien un stathme euclidien et $\mathbb{Z}[i]$ est bien euclidien.

Lemme 6. σ est stable par multiplication.

Preuve. Soit $n, m \in \sigma$, $\exists x, y \in \mathbb{Z}[i]$ tel que n=N(x) et m=N(y).
On a $nm = N(xy)$ donc $nm \in \sigma$

Lemme 7. Si p est premier tel que p = 3 mod 4 alors $p \notin \sigma$.

Preuve. Par l'absurde supposons que $p \in \sigma$ on a donc qu'il existe $a, b \in \mathbb{Z}$ tel que $p = a^2 + b^2$.
Par énumération des quatres cas de congruences possibles pour a et b on a a^2=0 mod 4 ou a^2=1 mod 4 de même pour b^2. Ce qui est impossible par hypothèse sur p.
Donc $p \notin \sigma$.

Lemme 8. Soit p premier. Alors $p \in \sigma$ si et seulement si p n'est pas irréductible dans $\mathbb{Z}[i]$.

Preuve. Si $p \in \sigma$ alors $p = a^2 + b^2$ avec $a, b \in \mathbb{Z}$
Alors $p = (a + ib)(a - ib) \in \mathbb{Z}[i]$ donc (a+ib) et (a-ib) non inversible car on a a et b non nuls sinon p est un carré.
Donc p est un produit de deux non inversible il n'est pas irréductible.

Supposons p non irréductible, il existe z et u non inversible tel que p=zu.
Ainsi, N(p)=p^2 et N(p)=N(zu)=N(z)N(u) et aucun des deux termes n'est égal à 1.
Donc N(z)=N(u)=p donc $p \in \sigma$

e.2 Le théorème de Fermat

Théorème 9. (Théorème des deux carrés de Fermat) Soit n un entier non nul. Alors $n \in \sigma$ si et seulement si $v_p(n)$ est pair pour tout p premier tel que p=3 mod 4.

Preuve. Supposons $v_p(n)$ pair pour tout p premier congru à 3 modulo 4.
Le but est de montrer que $v_p(n) \in \sigma$ pour tout p premier et on déduira que $n \in \sigma$ par stabilité multiplicative de σ.

Soit p premier tel que p = 3 mod 4. alors $p^{v_p(n)} = (p^{\frac{v_p(n)}{2}})^2 \in \sigma$.
Soit p=2 (mod 4) ou p= 1 (mod 4) donc il existe $a \in \mathbb{Z}$ tel, que $-1 = a^2 (\text{mod } 2)$.
Donc p divise a^2+1=(a+i)(a-i) on obtient une contradiction et donc p n'est pas premier dans $\mathbb{Z}[i]$ or $\mathbb{Z}[i]$ est euclidien.
Donc p n'est pas irréductible donc $p \in \sigma$ donc $n \in \sigma$.

Supposons que $n \in \sigma$ il existe a et b deux entiers relatifs tel que $n = a^2 + b^2$.
Soit p diviseur premier de n tel que p=3 mod 4 alors $p \notin \sigma$.
Donc p est irréductible donc premier.
Mais p divise n et n=(a+ib)(a-ib) donc donc p divise (a+ib) ou p divise (a-ib) dans $\mathbb{Z}[i]$.
Donc p divise a ou p divise b.
Donc $\frac{n}{p^2} = (\frac{a}{p})^2 + (\frac{b}{p})^2$ d'où p^2 divise n et $\frac{n}{p^2} \in \sigma$.
On itère le processus jusqu'à ce que p ne divise plus $\frac{n}{p^{2k}}$.
Donc $n = p^{2k}u$ avec u non divisible par p.
Donc $v_p(n) = 2k$ est pair.

f Références

- D. Perrin : Cours D'algèbre
- M. Aigner et G M. Ziegler : Raisonnements divins : Quelques démonstrations mathématiques particulièrement élégantes.
- R. Rashed : Histoire de l'analyse diophrantienne classique : D'Abu Kamil à Fermat.
- A. Szipirglas et AL : Mathématiques L3 : Algèbre- Cours complet avec 400 test et exercice corrigés.