**MP* - Anneaux principaux**

**Tous les anneaux dans la suite sont supposés commutatifs.** Les démonstrations de résultats très faciles sont laissées au lecteur.

**Définition 1:** : Soit $A$ un anneau.
Un idéal de $A$ est une partie $I$ de $A$ telle que:
• $(I, +)$ est un sous-groupe de $(A, +)$.
• $\forall a \in I, \forall b \in A$, $ab \in I$.

Si $A$ est un anneau et $a_1, ..., a_n \in A$, $a_1A + ... + a_nA = \{a_1b_1 + ... + a_nb_n \mid b_1, ..., b_n \in A\}$ est facilement un idéal, dit idéal engendré par $a_1, ..., a_n$.

On vérifie immédiatement la propriété:

**Propriété 1:** Une intersection d'idéaux d'un anneau $A$ est un idéal de $A$.

Rappelons un résultat déjà vu:

**Propriété 2:**

1. Si $K$ est un corps commutatif, les idéaux de $K[X]$ sont du type $AK[X]$, $A \in K[X]$.

2. Les idéaux de $\mathbb{Z}$ sont du type $a\mathbb{Z}$, $a \in \mathbb{Z}$. (Dans $\mathbb{Z}$, il y a coïncidence entre idéal et sous-groupe)

**Propriété 3:** Le noyau d'un morphisme d'anneaux est un idéal de l'anneau de départ.
La vérification est immédiate.

**A partir de maintenant, en plus d'être commutatifs, les anneaux sont supposés intègres.**

**Définition 2:** Soit $A$ un anneau, et $a, b \in A$. On dit que $a$ divise $b$ si et seulement si il existe $c \in A$ tel que $b = ac$, ie si et seulement si $b \in aA$.

On va s'intéresser à certains types d'anneaux dans lesquels il y a une arithmétique, comme dans $K[X]$ ou $\mathbb{Z}$, ie une notion d'irréductibles, et un théorème de décomposition.

**Définition 3:** : Un anneau $A$ est dit principal si tout idéal de $A$ est du type $aA$, $a \in A$.

Ainsi $K[X]$ et $\mathbb{Z}$ sont des anneaux principaux.

Un autre exemple: On pose $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ (entiers de Gauss). C'est facilement un sous-anneau de $\mathbb{C}$.
Cet anneau a été introduit par Gauss pour étudier l'équation $x^2 + z^2 = y$, $x, y, z \in \mathbb{Z}$, car $x^2 + y^2 = (x + iy)(x - iy)$.

**Propriété 4:** $\mathbb{Z}[i]$ est principal.

**Démonstration:**
Il y a dans $\mathbb{Z}[i]$ une espèce de division euclidienne (non unique):
Soient $x, y \in \mathbb{Z}[i]$, $y \neq 0$.
$\mathbb{Z}[i]$ est un réseau, de côtés de longueur 1. De ce fait (dessin), il existe $q \in \mathbb{Z}[i]$ tel que

$|q - x/y| \leq \frac{1}{\sqrt{2}} < 1$ (demi diagonale d'un carré de côté 1).
On se donne un tel $q$.
Soit $r = x - yq$. $r \in \mathbb{Z}[i]$.
De plus $|r| = |y||q - x/y| < |y|$.

Soit maintenant $I$ un idéal de $\mathbb{Z}[i]$. Si $I = \{0\}$, $I = 0\mathbb{Z}[i]$.
Supposons donc $I \neq 0$.
$\mathbb{Z}[i]$ est discret, donc $I$ aussi, donc on peut se donner $a \in I \backslash \{0\}$ de module minimal.
Comme $I$ est un idéal, $a\mathbb{Z}[i] \subset I$.
Inversement, soit $b \in I$. On écrit $b = aq + r$ avec $q, r \in \mathbb{Z}[i]$, $|r| < |a|$.
$r = b - aq$ et $a, b \in I$, donc $r \in I$.
Du fait de la minimalité de $|a|$, $r = 0$ et $b = aq \in a\mathbb{Z}[i]$. ♣

$\mathbb{Z}[i]$ possédant une division euclidienne, on dit que $\mathbb{Z}[i]$ est euclidien, ce qui est plus fort que principal.

**Propriété 5:** $\mathbb{Z}[i]^{\times} = \{1, -1, i, -i\}$
**Démonstration:** Si $a, b \in \mathbb{Z}$, on pose $N(a + ib) = |a + ib|^2 = a^2 + b^2 \in \mathbb{N}$.
Si $xy = 1$, $x, y \in \mathbb{Z}[i]$, $N(xy) = N(x)N(y) = 1$, donc $N(x) = 1$, donc $x \in \{-1, 1, -i, i\}$.
De plus $-1, 1, -i, i$ sont inversibles d'inverses $-1, 1, i, -i$. ♣.

**Définition 4:** Soit $A$ un anneau. $x \in A$ est dit irréductible si et seulement si $x$ est non nul, n'est pas inversible, et pour tous $y, z \in A$, si $x = yz$, alors $y$ ou $z$ est inversible.
$x, y$ sont dits associés si et seulement si il existe $z$ inversible tel que $x = yz$.

Ainsi les irréductibles de $\mathbb{Z}$ sont les nombres premiers et leurs opposés.

*Ce qui suit n'est pas au programme, mais bon à connaître pour X/ENS.*

**Définition 5:** Soient $a_1, ..., a_n \in A$, $A$ étant principal. $a_1A + ... + a_nA$ qui est un idéal s'écrit $cA$.
Tout $c \in A$ tel que $cA = a_1A + ... + a_nA$ est appelé un pgcd de $a_1, ..., a_n$.
Notons que si $c$ est un pgcd, $a_i = a_1 \times 0 + ... + a_i \times 1 + ... + a_n \times 0 \in a_1A + ... + a_nA = cA$, donc $c|a_i$.

**Propriété 6:** Si $aA = bA$ si et seulement si $a$ et $b$ sont associés, et donc si $A$ est principal, et $c$ est un pgcd de $a_1, ..., a_n$, les autres sont les éléments associés à $c$.
**Démonstration:** Si $c$ est inversible, $x = cc^{-1}x$, donc $cA = A$, et donc $acA = aA$, d'où $\Leftarrow$.
Inversement, si $aA = bA$ avec $b \neq a$: $a \in bA$, et $b \in aA$, donc il existe $x, y \in A$ tels que $a = bx$ et $b = ay$.
Disons $a \neq 0$. On a $a(1 - xy) = 0$ donc par intégrité $xy = 1$, et donc $x, y$ sont inversibles, et $a$ et $b$ associés. ♣

**Propriété 7:** $A$ est principal. Si $a, b \in A$ sont irréductibles, soit ils sont associés, soit 1 est un pgcd de $a$ et $b$.
**Démonstration** $a, b$ irréductibles. Supposons que $a$ et $b$ ne sont pas associés.
Soit $c$ un pgcd de $a$ et $b$. $cA = aA + bA$.
$c|a$, $c|b$, donc on se donne $x, y$ tels que $a = cx$ et $b = cy$.
Si $c$ n'était pas inversible, comme $a$ et $b$ sont irréductibles, $x, y$ sont inversibles, et alors $a = b(y^{-1}x)$, et $a$ et $b$ sont associés, ce qui est absurde.
Donc $c$ est inversible, et donc $1 = cc^{-1}$ qui est associé à $c$ est aussi un pgcd de $a$ et $b$.

**Propriété 8:** Lemme de Gauss.
$A$ est principal. Soient $x, y, z \in A$ tels que $x$ divise $yz$ et $x$ est premier à $y$, ie 1 est un pgcd de $x$

et $y$.
Alors $x$ divise $z$.
**Démonstration:** On a $xA+yA=1A=A$. On peut donc se donner $u,v\in A$ tels que $xu+vy=1$. Alors $z=xuz+vyz$ est divisé par $x$ car $x|yz$. ♣

**Propriété 9:** Théorème de décomposition.
$A$ est principal. Soit $a\in A$ non inversible et non nul.
Alors il existe $b_1,...,b_n$ irréductibles tels que $a=b_1...b_n$.
De plus, si $c_1,...,c_k$ sont d'autres irréductibles tels que $a=c_1...c_k$, alors $k=n$, et quitte à renuméroter, $c_i$ est associé à $b_i$ pour tout $i$.
**Démonstration**:
**Existence:** Soit $a\in A$ non inversible et non nul.
Si $a$ est irréductible, $n=1$. $a$ est décomposé.
Sinon, on peut se donner $b_1,b_2$ non inversibles tels que $a=b_1b_2$.
Si $b_1$ et $b_2$ admettent des décompositions, c'est fini.
Sinon, disons que $b_1$ n'admet pas de décomposition. $b_1$ étant alors non irréductible, on écrit $b_1=c_1c_2$ avec $c_1c_2$ non inversibles.
$b_1$ étant non décomposable, $c_1$ ou $c_2$ ne l'est pas, disons que $c_1$ ne l'est pas.
etc...
On forme ainsi une suite croissante d'idéaux: $...c1|b_1|a$, ce qui donne $aA\subset b_1A\subset c_1A\subset ...$, et en fait strictement croissante:
Si on avait $aA=b_1A$, $a$ et $b_1$ seraient associés: on se donne $x$ inversible tel que $a=b_1x$.
Alors $b_1b_2=b_1x$, et $b_1\neq 0$, donc par intégrité $x=b_2$ ce qui est absurde car $b_2$ est non inversible.
Ainsi $aA\neq b_1A$. Il en est de même pour la suite.
En renommant les choses, on a donc $(d_nA)_{n\in N}$ une suite strictement croissante d'idéaux.
Notons $I=\bigcup\limits_{n\in\mathbb{N}} d_nA$.
$I$ est un idéal car si $x,y\in I$, il existe $n1,n2$ tels que $x\in d_{n_1}A$, $y\in d_{n_2}A$, et avec $n=\max(n_1,n_2)$, $x,y\in d_nA$, et donc $x+y,-x\in d_nA\subset I$, et si $z\in A$, $zx\in d_nA\subset I$.
On peut donc se donner $e\in A$ tel que $eA=\bigcup\limits_{n\in\mathbb{N}} d_nA$.
Alors, il existe $N$ tel que $e\in d_NA$, ce qui implique que $eA\subset d_NA$ ie $I\subset d_NA$. Mais alors $d_NA=I$, et donc $\forall n\geq N$, $I\subset d_nA\subset I$, ie $d_nA=I$, ce qui contredit la stricte croissance.

**Unicité aux inversibles près:**
Supposons $a=b_1...b_n=c_1...c_k$ avec $\forall i,\ b_i,c_i$ irréductibles.
Si $b_1$ n'est pas associé à $c_1$, par la propriété 7, $b_1$ est premier à $c_1$, et alors divise $c_2...c_k$ par le lemme de Gauss.
Puis, si $b_1$ n'est pas associé à $c_2$, $b_1$ divise $c_3...c_k$.
Au pire, on finit par $b_1|c_1$. Mais alors, comme $c_1$ est irréductible, et $b_1$ non inversible, $c_1=b_1x$ avec $x$ inversible.
Ainsi $b_1$ est associé à un $c_i$, disons $c_1$. On écrit $b_1=c_1\varepsilon$, $\varepsilon$ inversible.
Par intégrité on simplifie: $(\varepsilon b_2)b_3...b_n=c_2...c_k$. $\varepsilon b_2$ est irréductible.
Et on recommence... ♣

Donnons un exemple de l'utilisation de l'arithmétique dans $\mathbb{Z}[i]$: le théorème des deux carrés:

**Propriété 10:** Soit $n\geq 2$ un entier.
Alors $n$ est somme de deux carrés d'entiers si et seulement si pour tout nombre premier $p$ divisant $n$ et congru à $3[4]$, $v_p(n)$ est pair.

Nous allons décomposer la démonstration en plusieurs propriétés. Dans la suite, carré signifie carré d'entier.

**Propriété 11:** Un entier $n \in \mathbb{N}$ est somme de deux carrés si et seulement si il existe $x \in \mathbb{Z}[i]$ tel que $n = N(x)$ ($N$ définie dans la propriété 5).
Un produit de somme de deux carrés est une somme de deux carrés.
**Démonstration:** La première assertion est triviale, et pour la seconde, on note que $N(x)N(y) = N(xy)$. ♣

On rappelle la propriété vue en exercice:

**Propriété 12:** Soit $p$ un nombre premier $\geq 3$. Alors $-1$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p \equiv 1[4]$.

**Propriété 13:** Soit $p$ un nombre premier congru à 1 modulo 4. Alors $p$ est somme de deux carrés.
**Démonstration:** Nous allons utiliser $\mathbb{Z}[i]$.
On se donne donc $p$ premier $\equiv 1[4]$.
Alors $-1$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$.
Ainsi, il existe $a \in \mathbb{N}$ tel que $-1 \equiv a^2[p]$.
Alors $p$ divise $a^2 + 1 = (a+i)(a-i)$ dans $\mathbb{Z}$, donc a fortiori dans $\mathbb{Z}[i]$.
Soit $d$ un pgcd de $p$ et $a+i$ dans $\mathbb{Z}[i]$.
$d$ divise $p$ dans $\mathbb{Z}[i]$, donc $N(d)$ divise $N(p) = p^2$ dans $\mathbb{N}$, donc $N(d) \in \{1, p, p^2\}$.
On examine les 3 cas.
Si $N(d) = 1$: $d$ est inversible dans $\mathbb{Z}[i]$, donc $p$ et $a+i$ sont premiers entre eux, donc par le lemme de Gauss, $p$ divise $a-i$.
On écrit alors $a - i = p(c+id)$, $c, d \in \mathbb{Z}$. Alors $pd = -1$, absurde.
Si $N(d) = p^2$: $d|p$ On écrit $p = xd$, $x \in \mathbb{Z}[i]$. $p^2 = N(p) = N(x)N(d) = N(x)p^2$, donc $N(x) = 1$, et $x \in \{1, -1, i, -i\}$ est inversible. $d$ et $p$ sont associés.
Donc $d|a+i$ donne $p|a+i$, ce qui est impossible comme $p|a-i$ dans le cas précédent.
Finalement $N(d) = p$, ce qui donne que $p$ est somme de carrés d'entiers. ♣.

A partir de là, notant que $2 = 1^1 + 1^2$ et $a^2 = a^2 + 0^2$, en combinant les propriétés 11 et 13, on a le sens $\Leftarrow$ de la propriété 11.

Concernant le sens $\Longrightarrow$, si $n = a^2 + b^2$, et $p$ est premier $\equiv 3[4]$ divise $n$:
On écrit $n = a^2 + b^2$. En passant aux classes dans $\mathbb{Z}/p\mathbb{Z}$, $\bar{a}^2 + \bar{b}^2 = 0$. Si $\bar{a} \neq 0$, on a $-1 = (\bar{b}\bar{a}^{-1})^2$, ce qui contredit la propriété 12. donc $\bar{a} = 0$. De même $\bar{b} = 0$.
Alors $p|a$, $p|b$, $p^2|n$, et on simplifie $n = a^2 + b^2$ par $p^2$: $(n/p^2) = (a/p)^2 + (b/p^2)$.
Et on recommence.
Si $v_p(n) = 2k+1$ est impair, en $k$ étapes, on aboutit à $m := n/p^{2k}$ est somme de deux carrés, et $v_p(m) = 1$.
$m = a^2 + b^2$, on passe dans $\mathbb{Z}/p\mathbb{Z}$ comme précédemment, ce qui donne que $p^2|m$ ce qui est absurde.
Ainsi $v_p(n)$ est pair.