Exercice 28.

Soit A un anneau fini. Soit $P < A$ idéal premier.

Montrer que P est un idéal maximal.

Rappel. P est un idéal premier si $P \neq A$ et si $\forall x, y \epsilon A, xy \epsilon P \Rightarrow x$ ou $y \epsilon P$.

$\Leftrightarrow$l'anneau quotient A/P est intègre.

P est maximal si pour tout idéal $P \leqslant I \leqslant A$, on a $I = P$ ou A.

$\Leftrightarrow$l'anneau quotient A/P est un corps.

Donc maximal$\Rightarrow$premier mais en général premier $\not\Rightarrow$maximal : exemple 0 est premier mais non maximal dans $\mathbb{Z}$.

Indication : raisonner avec A/P. Vérifier qu'un anneau intègre fini est un corps.

A fini$\Rightarrow A/P$ est fini. Or un anneau intègre fini est un corps.

En effet si A' est un anneau intègre fini, alors pour tout $0 \neq a \epsilon A'$, l'application :

$A' \to A'$ $x \mapsto ax$ est injective $\Rightarrow$surjective. Donc il existe x tel que $ax = 1$.

a inversible!.

Si A est fini, si $P < A$ est premier, alors A/P est intègre fini$\Rightarrow$corps$\Rightarrow A/P =$ corps$\Rightarrow P$ maximal.

Exercice 29.

Soit A idéal, soit $M < A$ idéal maximal. Si $M^n \leqslant P$ et P idéal premier, alors $P = M$.

Il suffit de montrer que $M \leqslant P$ car M idéal maximal. Soit $x \epsilon M$. Alors $x^n \epsilon P$.

Comme P premier, $x^n \epsilon P \Rightarrow x \epsilon P$.

En effet $x^n \epsilon P \Leftrightarrow x^n = 0$ dans A/P. Or A/P est intègre donc $x^n = 0$ dans $A/P \Rightarrow x =$ 0dans A/P c-à-d $x \epsilon P$.

Ou bien : P premier signifie que $x, y \notin P \Rightarrow xy \notin P$ en particulier, $x \notin P \Rightarrow x^n \notin P$.

C'est vrai pour tout $x \epsilon M$ donc $M \leqslant P$.

Exemple : si $p|27$, alors $p=3$. $(M=(3),\ n=3,\ P=(p))$

Exercice 30.

Cardinal de $\mathbb{Z}[\sqrt{d}]/(m)$. On suppose d entier sans facteur carré. Si $d=c^2d'$, alors $\sqrt{d}=c\sqrt{d'} \Rightarrow \mathbb{Z}[\sqrt{d}]=\mathbb{Z}[\sqrt{d'}]$

$\mathbb{Z}[\sqrt{d}]=\mathbb{Z}\oplus\mathbb{Z}\sqrt{d}=\{a+b\sqrt{d}: a,b\epsilon\mathbb{Z}\}$.

$(m)=\{m.(a+b\sqrt{d}): a,b\epsilon\mathbb{Z}\}=\{ma+mb\sqrt{d}: a,b\epsilon\mathbb{Z}\}$

$a+b\sqrt{d}\epsilon(m) \Leftrightarrow m|a$

et $m|b$.

$\mathbb{Z}[\sqrt{d}]/(m) \leftrightarrow (\mathbb{Z}/m\mathbb{Z})^2$ bijection !

$a+b\sqrt{d} \bmod m \leftarrow\!\shortmid (a,b)$

Donc $|\mathbb{Z}[\sqrt{d}]/(m)|=m^2$.

Ex. $|\mathbb{Z}[\sqrt{2}]/(3)|=9$. $(\mathbb{Z}[\sqrt{2}]/(3)=\mathbb{F}_9)$.

(2) est premier dans $\mathbb{Z}[\sqrt{d}] \Leftrightarrow\ \mathbb{Z}[\sqrt{d}]/(2)$ est intègre.

1er cas : d pair. $0 \neq \sqrt{d}$ dans $\mathbb{Z}[\sqrt{d}]/(2)$. Mais $\sqrt{d}^2=d=0$ dans $\mathbb{Z}[\sqrt{d}]/(2)$.

Donc non intègre !

2ème cas : d est impair , alors : $d-1=0\ \mathbb{Z}[\sqrt{d}]/(2) \Rightarrow (d-1)=\underbrace{(\sqrt{d}-1)}_{\neq 0}(\underbrace{\sqrt{d}+1}_{\neq 0})$

donc l'anneau $\mathbb{Z}[\sqrt{d}]/(2)$n'est pas intègre.

Donc 2 n'est pas premier dans $\mathbb{Z}[\sqrt{d}]$.

Exercice 31.

1)

$I, J \leqslant A$. $\pi_I: A \to A/I\ a \mapsto a+I$.

$\bar{J}=\pi_{_I}(J)$

$\pi_{_I}$ surjectif $\Rightarrow \pi_{_I}(J)$=idéal de A/I. En effet, si $\bar{a}\epsilon A/I$, si $x\epsilon J$, alors $\bar{a}\pi_I(x)=\pi_{_I}(ax)\epsilon\bar{J}$.

2) $A/I/_{\bar{J}}\cong A/(I+J)$

$I+J=\{x+y\colon x\epsilon I, y\epsilon J\}$

$A/(I+J)\to\ A/I/_{\bar{J}}$

$x+I+J\mapsto(x+I)+\bar{J}$

$x+I+J\leftarrow\!\shortmid(x+I)+\bar{J}$

Ces deux applications sont bien définies et sont réciproques l'une de l'autre (et ce sont des morphismes d'anneaux)

Corollaire. Comme $I+J=J+I$, on a : $A/I/_{\pi_{_I}(J)}\cong A/J/_{\pi_J(I)}$

Exemple . $\underset{A/J/\pi_J(I)}{\mathbb{Z}[\sqrt{2}]/(3)}\cong\underset{A/I/\pi_I(J)}{\mathbb{F}_3[X]/(X^2-2)}\cong\mathbb{Z}[X]/(3,X^2-2)$

$(A=\mathbb{Z}[X],\ I=(3),J=(X^2-2)\Rightarrow\mathbb{Z}[\sqrt{2}]/(3)$ est un corps).

$\pi_I(J)$ = l'idéal engendré par X^2-2 dans l'anneau $\mathbb{F}_3[X]$

$J=$ l'idéal engendré par X^2-2 dans $\mathbb{Z}[X]$.

Exercice 33.

1)

$(5,X^2+3)$ *n'est pas principal dans* $\mathbb{Z}[X]$.

Sinon : $\exists P(X)\epsilon\mathbb{Z}[X],(P)=(5,X^2+3)$ ...

$\Rightarrow 5\epsilon(P)\Rightarrow P\mid 5$ dans $\mathbb{Z}[X]\Rightarrow P(X)=$ constante $=\pm5$ ou ±1

Or $P\mid X^2+3$ dans $\mathbb{Z}[X]\Rightarrow P=\pm1$ (car 5 ne divise pas 1)

Donc $(P)=\mathbb{Z}[X]$. Or $(5,X^2+3)\neq\mathbb{Z}[X]$.

En effet, si $1=A(X)5+B(X)(X^2+3)$ avec A,B$\epsilon\mathbb{Z}[X]$, alors :

$1=A(i\sqrt{3})\times5=(a+i\sqrt{3}b)\times5$ pour certains $a,b\epsilon\mathbb{Z}\Rightarrow1=\underset{\epsilon\mathbb{Z}}{(a^2+3b^2)}\times5$ absurde.

$(X^2+1, X+2)$ *n'est pas principal dans* $\mathbb{Z}[X]$.

Sinon : il existerait $P \epsilon \mathbb{Z}[X]$ tel que $(P) = (X^2+1, X+2)$

$\Rightarrow P | X^2+1$ dans $\mathbb{Z}[X] \Rightarrow P = \pm 1$ ou $\pm(X^2+1)$.

Or $P | X+2 \Rightarrow P = \pm 1 => (X^2+1, X+2) = (1) = \mathbb{Z}[X]$

Maissi $1 = A(X)(X^2+1) + B(X)(X+2)$ avec $A, B \epsilon \mathbb{Z}[X] \Rightarrow 1 = A(-2) \times 5$ absurde !

$\boxed{(X^3-1, X^4-1) \text{ est principal dans } \mathbb{Z}[X]}$

$X^3-1 = (X-1)(X^2+X+1)$, $X^4-1 = (X-1)(X+1)(X^2+1)$

Si $(X^3-1, X^4-1) = (X-1)(X^2+X+1, (X+1)(X^2+1)) = (P)$ avec $P(X) \epsilon \mathbb{Z}[X]$

$\Rightarrow (X^2+X+1, (X+1)(X^2+1)) = (Q)$ où $Q = \frac{P}{X-1} \epsilon \mathbb{Z}[X]$.

$\Rightarrow Q = \pm 1$

Or, $(X+1)(X^2+1) = X(X^2+X+1) + 1$ donc

$(X^2+X+1, (X+1)(X^2+1)) = (1) \Rightarrow (X^3-1, X^4-1) = (X-1)$.

2) (application du n°30)

$(x, x+1) = (1) = \mathbb{Z}[x]$

ATTENTION : ce n'est pas un idéal propre.

$\mathbb{Z}[x]/(5, x^2+4) \cong \mathbb{F}_5[x]/(x^2+4) = \mathbb{F}_5[x]/(x^2-1) = \mathbb{F}_5[x]/((x-1)(x+1))$

$\cong \mathbb{F}_5[x]/(x-1) \times \mathbb{F}_5[x]/(x+1) \cong \mathbb{F}_5 \times \mathbb{F}_5$

donc non intègre (car $(1,0).(0,1) = (0,0)$) donc l'idéal $(5, x^2+4)$ n'est pas premier !

En effet $(x-1) = \ker\left(\underset{\mathbb{F}_5[x] \to \mathbb{F}_5}{P(x) \mapsto P(1)} \right) \Rightarrow \mathbb{F}_5[x]/(x-1) \cong \mathbb{F}_5$

$\mathbb{Z}[x]/(5, x^2+3) \cong \mathbb{F}_5[x]/(x^2+3) =$ corps à 25 éléments car x^2+3 est un polynôme irréductible sur $\mathbb{F}_5$. Donc $(5, x^2+3)$ est maximal dans $\mathbb{Z}[x]$.

$\mathbb{Z}[x]/(x^2+1, x+2) \cong \mathbb{Z}[x]/(x+2) \ /_{(x^2+1)} \cong \mathbb{Z}/(5) = \mathbb{Z}/5\mathbb{Z} =$ corps !

Donc $(x^2+1, x+2)$ est un idéal maximal de $\mathbb{Z}[x]$.