Fiche de révisions chapitre 4 : Anneau quotient.

• ~~Définition : Soit $(A,+,\times)$ un anneau. Par définition, $(A,+)$ est un groupe abélien. Par conséquent, $\forall$ sous groupe I de A, $(A/I,+)$ est un groupe pour l'opération $(r+I)+(s+I)=(r+s)+I$ $\forall r,s\in A$. $(r+I)*(s+I)=(r*s)+I$ $\forall r,s\in A$.~~

I) $(\mathbb{Z},+,\times)$

Soit A un anneau et I un sous ensemble de A. Alors I est un idéal de A si :
- I est un sous groupe de A.
- $\forall r\in A$ $\forall \alpha\in I$, $\alpha.r\in I$ et $r.\alpha\in I$.

• Propriété : Soit A un anneau commutatif.
Alors $\alpha.A=\{a.x \mid x\in A\}$ est un idéal de A qu'on notera (a)

• Théorème : Soit A un anneau et I un idéal de A (et $I\neq A$) Alors A/I muni des opérations :
$(r+I)+(s+I)=(r+s)+I$ $\forall r,s\in A$
$(r+I)*(s+I)=(r*s)+I$ $\forall r,s\in A$
forme un anneau dont le neutre $+$ est I et $\times$ est $1+I$.

En particulier, les classes $[a+n\mathbb{Z}]$ sont données par $\mathbb{Z}/n\mathbb{Z}$ avec $n\mathbb{Z}$ un idéal de $(\mathbb{Z},+,\times)$.

Dans $\mathbb{Z}/n\mathbb{Z}$, on dit que $[a+n\mathbb{Z}]$ est inversible si il existe une classe $\bar{b}$ tq

$$[a+n\mathbb{Z}]\times[b+n\mathbb{Z}]=[1+n\mathbb{Z}]$$
$$\Leftrightarrow [a\times b+n\mathbb{Z}]=[1+n\mathbb{Z}]$$
$$\Leftrightarrow [a\times b-1+n\mathbb{Z}]=[n\mathbb{Z}]$$
$$\Leftrightarrow a.b-1=-k.n$$
$$\Leftrightarrow \underline{a.b+k.n=1}$$

⚠ $[a+n\mathbb{Z}]$ inversible $\Leftrightarrow PGCD(a,n)=1$.

II) $(F[x],+,\times)$

• L'ensemble des classes est $\{[T(x)+(P(x))] \mid T(x)\in F[x]\}$ noté $F[x]/(P(x))$ avec $F[x]$ anneau et $(P(x))$ un idéal.

• Pour retrouver le représentant du degré minimal $\frac{F[x]}{((P(x))}=\{r(x) \mid r(x)\in F[x],\ \deg r<\deg P\}$

ex : $(\mathbb{R}[x]/(x^2+1),+,\times)\rightarrow[a+bx+(x^2+1)]$

• Si F est un corps commutatif fini alors $\left|\left(\frac{F[x]}{(P(x))},+,\times\right)\right|=|F|^{\deg P}$

• Le groupe multiplicatif A^* d'un anneau $(A,+,\times)$ est l'ensemble de ses éléments inversibles.

• $\left(\frac{F[x]}{(P(x))}\right)^*$ est cyclique si P irréductible et F fini.

• $\frac{F[X]}{(P(X))}$ est un champ (corps commutatif) si $F[X]$ est un $P(x)$ est irréductible