Feuille de TD 6 CORPS

Exercice 1.

Soit A un anneau. Soit K corps tel que $K \subset A$.

Alors A est un $K-$ espace vectoriel.

En effet, $(A,+)$ est un groupe commutatif.

$\forall \lambda, \mu \epsilon K$, $\forall a, b \epsilon A$, $(l+\mu)a = \lambda a + \mu a$, $\lambda(a+b) = \lambda a + \lambda b$.

Et $1.a = a$.

On suppose que A est de dimension finie sur K.

Alors A est un corps.

En effet, pour tout $0 \neq a \epsilon A$, l'endomrphisme $K-$linéaire :

$A \to A, x \mapsto a\,x$

est injectif $\Rightarrow$surjectif.

Donc il existe $b \epsilon A$ tel que $a\,b = 1$ ...

Exercice 2.

Soit K corps de cardinal 4.

Alors $(K,+) \ncong \mathbb{Z}/4\mathbb{Z}$ mais $(K,+) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

$\varphi : \mathbb{Z} \to K$, $n \mapsto \underbrace{1 + \cdots + 1}_{n \text{fois}}$ est un morphisme d'anneaux !

$\ker \varphi =$ idéal premier de $\mathbb{Z}$ car $\mathbb{Z}/\ker \varphi \cong \varphi(\mathbb{Z}) =$ sous-anneau de K donc intègre ! de cardinal qui divise $4 = |K|$.

Donc $\ker \varphi = 2\mathbb{Z}$. Donc K est de caractéristique 2.

Donc dans K, $1+1=0$. Donc dans K, $x+x=0 (\forall x \epsilon K)$.

Donc $K \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Plus généralement que si K est un corps fini de cardinal p^n pour un $n \epsilon \mathbb{N}_{>0}$, alors $(K,+) \cong (\mathbb{Z}/p\mathbb{Z})^n$.

Exercice 3.

Soit K un corps de caractéristique p.

C-à-d. : $\forall x \epsilon K$, $\underbrace{x + \cdots + x}_{p \text{ fois}} = p.x = 0$.

1°) $\sigma : K \to K, x \mapsto x^p$ est un morphisme d'anneaux.

Il suffit de vérifier : $\forall x, y \epsilon K$, $(x+y)^p = x^p + y^p$.

En effet, $(x+y)^p = x^p + \sum_{k=1}^{p-1} \underbrace{\binom{p}{k}}_{=0 \bmod p} x^{p-k} y^k + y^p$. Or $\binom{p}{k}$ est un multiple de p pour tout $1 \leqslant k \leqslant p-1$.

2°) Si $K = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, alors $\sigma = \mathrm{Id}$.

$\forall x \epsilon \mathbb{F}_p$, $x^p = x$. En effet, c'est évident si $x = 0$. Si $x \neq 0$, alors $x \epsilon \mathbb{F}_p^\times$ et comme $|\mathbb{F}_p^\times| = p-1$, $x^{p-1} = 1 \Rightarrow x^p = x$.

3°) Comme σ est un morphisme de corps, c'est forcément injectif !

(car le noyau de σ est un idéal$\Rightarrow$0).

En effet : soit I un idéal de K. si $0 \neq x \epsilon I$ alors $x^{-1}x = 1 \epsilon I \Rightarrow I = K$. Donc si I est un idéal de K (corps), alors $I = 0$ ou $I = K$.

Or $\sigma : K \to K$, K fini $\Rightarrow$injectif$\Leftrightarrow$surjectif$\Leftrightarrow$isomorphisme.

4°) Contre-exemple. $K = \mathbb{F}_p(X)$ corps des fractions rationnelles en une variable.

$K \to K$, $f \mapsto f^p$ est un morphisme de corps d'image $\mathbb{F}_p(X^p) \underset{\neq}{\subset} \mathbb{F}_p(X)$.

Donc non surjectif.

Exercice : $\mathbb{F}_3(X)^\times \cong \mathbb{Q}^\times$ comme groupes. *Indication : $\mathbb{F}_3[X]^\times$ et $\mathbb{Z}^\times$ sont d'ordre 2 et il y a une bijection (non explicite) entre les irréductibles de $\mathbb{F}_3[X]$ et* ceux de $\mathbb{Z}$.

Exercice 4.

$A = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$,

1)$A=\{0,1,a,b\}$ Dans A : $x+x=0\Leftrightarrow x=-x$.

$a+b=0$ ou $\underbrace{1}_{\text{seule possibilité}}$ ou a ou b

$a+b\neq b, a+b\neq a, a+b\neq 0$ car sinon $a=-b=b$.

2)Si $a^2=0$.

$(a+b)^2=1=a^2+b^2\Rightarrow b^2=1$.

$ab=0\Rightarrow a=ab^2=0b=0$ absurde.

Donc $ab=a$.

3°)Si $a^2\neq 0\neq b^2$, alors $a^2=a\Leftrightarrow a(a-1)=0$. Or $a-1=-b=b$.

Donc $a^2=a\Leftrightarrow ab=0$.

De même $b^2=b$.

Voici l'isomorphisme :

$A\to\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$

$0\mapsto(0,0)$

$1\mapsto(1,1)$

$a\mapsto(1,0)$

$b\mapsto(0,1)$

À l'aide des questions précédentes, on vérifie que c'est un (iso)morphisme d'anneaux.

4°) Si $a^2, b^2, ab\neq 0$, alors A est intègre. (Car un produit de deux éléments non nuls est non nul).

Or intègre + fini $\Rightarrow$ corps.

On a $a^2=1$ ou a ou b.

Or $a^2=1\Leftrightarrow(a-1)^2=0\Leftrightarrow a=1$ absurde.

$a^2=a\Leftrightarrow(a-1)a=0\Leftrightarrow a=1$ ou 0. absurde.

Donc $a^2 = b$. De même $b^2 = a$. De même $ab = 1$.

5) Il s'agit de vérifier qu'il y a un seul tableau d'addition et un seul tableau de multiplication.

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\times$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Autrement dit si $K = \{0, 1, a, b\}$ et $K' = \{0, 1, a', b'\}$ sont des corps à 4 éléments, alors on a un isomorphisme $K \cong K' a \mapsto a'$, $b \mapsto b'$.

Plus généralement, à isomorphisme près il existe un unique corps de cardinal q si q est une puissance d'un nombre premier.

Exercice 5.

$L = \mathbb{F}_2[X]/(X^2 + X + 1)$

1) $L = \text{corps} \Leftrightarrow (X^2 + X + 1)$ est maximal (comme idéal) dans $\mathbb{F}_2[X] \Leftrightarrow X^2 + X + 1$ est irréductible sur $\mathbb{F}_2$. C'est le cas car pas de racine et de degré 2.

Rappel. Proposition. Si K corps. Si $P(X) \epsilon K[X]$, alors $K[X]/(P)$ est un K-espace vectoriel de dimension $\deg P$ (car une base est donnée par $1, X, \ldots,$ $X^{d-1} \bmod P$ o ù $d = \deg P$).

Donc $L = \mathbb{F}_2$-espace vectoriel de dimension 2. Donc $\cong \mathbb{F}_2^2$ (comme groupe)$\Rightarrow$cardinal $= 2^2 = 4$.

Pour les tables, posons $a = X \bmod P$, $b = 1 + X \bmod P$. Cf la fin de l'exo précédent.

2) déjà fait.

3) $\mathbb{F}_2[X]/(X^2+1) \cong \mathbb{F}_2[X]/((X+1)^2) \overset{*}{\cong} \mathbb{F}_2[X]/(X^2)$ un anneau avec un élément nilpotent non nul : $X \bmod X^2$. (Ce n'est pas $\mathbb{F}_2 \times \mathbb{F}_2$ comme anneau)

$P(X) \mapsto P(X-1)$

* :

L'isomorphisme $\mathbb{F}_2[X] \to \mathbb{F}_2[X], P(X) \mapsto P(X-1)$ envoie $(X+1)^2$ sur $(X)^2$

Exercice 7.

$\mathbb{R}[X]/(X^2+X+1) \cong \mathbb{C}$.

$P(X) \mapsto P\left(\frac{-1+i\sqrt{3}}{2}\right)$

Si $j = \frac{-1+i\sqrt{3}}{2}$, alors $P(j)=0 \Rightarrow P(\bar{j})=0 \Rightarrow (X-j)(X+j) = X^2+X+1 | P(X)$.

Donc ce morphisme est injectif donc surjectif pour des raisons de dimension.

Exercice. Si p est un nombre premier impair,

alors $\mathbb{Z}[i]/p \cong \mathbb{F}_{p^2}$ si $p = 3 \bmod 4$ et $\mathbb{Z}[i]/p \cong \mathbb{F}_p \times \mathbb{F}_p$ si $p = 1 \bmod 4$.

Indication : $\mathbb{Z}[i]/p \cong \mathbb{Z}[X]/(X^2+1, p) \cong \mathbb{F}_p[X]/(X^2+1)$.

Exercice 8.

Si $K < L$ sont des corps. Alors L est un $K-$espace vectoriel. Et on note $[L\colon K]$ la dimension.

1.– Si $L = K[x]$, si $P(X) \epsilon K[X]$ est le polynôme minimal de x sur K, alors $K[x] \cong K[X]/(P)$ donc $[L\colon K] = \deg P$.

2.– Si $K_1 < K_2 < K_3$, alors $[K_3\colon K_1] = [K_3\colon K_2][K_2\colon K_1]$.

$[\mathbb{C}\colon \mathbb{R}] = 2$

$[\mathbb{Q}(\sqrt{2})\colon \mathbb{Q}] = 2$ car le polynôme minimal de $\sqrt{2}$ sur $\mathbb{Q}$ est X^2-2.

$\left[\mathbb{Q}\left(\sqrt[3]{2}\right)\colon \mathbb{Q}\right] = 3$ car le polynôme minimal de $\sqrt[3]{2}$ sur $\mathbb{Q}$ est X^3-2

(car X^3-2 annule $\sqrt[3]{2}$ et est irréductible sur $\mathbb{Q}$).

$$[\mathbb{Q}(\sqrt{2}, i)\colon \mathbb{Q}] = \underbrace{[\mathbb{Q}(\sqrt{2})(i)\colon \mathbb{Q}(\sqrt{2})]}_{2}\underbrace{[\mathbb{Q}(\sqrt{2})\colon \mathbb{Q}]}_{2} = 4$$

Le polynôme $X^2+1 \epsilon \mathbb{Q}(\sqrt{2})[X]$ annule i et est irréductible (pas de racine !)

Donc c'est le polynôme minimal de i sur $\mathbb{Q}(\sqrt{2})$.

Exercice. On peut en déduire : $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(i+\sqrt{2})$.

Exercice 9.

$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$?

$\geqslant$: facile.

$\leqslant$: *indication* = calculer $\frac{1}{\sqrt{2}+\sqrt{3}} = \sqrt{3}-\sqrt{2}$

En déduire que $\sqrt{3} = \frac{1}{2}\Big(\sqrt{2}+\sqrt{3}+\frac{1}{\sqrt{2}+\sqrt{3}}\Big) \epsilon \mathbb{Q}(\sqrt{2}+\sqrt{3})$

$\sqrt{2} = \frac{1}{2}\Big(\sqrt{2}+\sqrt{3}-\frac{1}{\sqrt{2}+\sqrt{3}}\Big) \epsilon \mathbb{Q}(\sqrt{2}+\sqrt{3})$ ...