ALGÈBRE COMMUTATIVE

Feuille de td 5

corrections

Exercice 1.

Soit $P(X)=X^4-X-1$.

1.– Le polynôme P est irréductible sur $\mathbb{F}_2$ doncest irréductible sur $\mathbb{Q}$.

D'après le tableau de variations de la fonction réelle $\mathbb{R}\to\mathbb{R}, x\mapsto P(x)$, on voit que P s'annule exactement deux fois sur $\mathbb{R}$.

Posons $P(X)=(X-x_1)(X-x_2)(X^2+a'X+b')$ et $X^2+aX+b=(X-x_1)(X-x_2)$. Avec a, a',b,b' réels. Coefficient devant $X^3=0=a+a'\Rightarrow a'=-a$.

2.– Comme $P(X)=(X^2+aX+b)(X^2-aX+b')=X^4-X-1$, on a :

coefficient devant $X^2=0=b-a^2+b'$;

coefficient devant $X=-1=ab'-ba=a(b'-b)$;

coefficient constant $=-1=bb'$.

Donc $\begin{cases} b+b'=a^2 \\ b-b'=\frac{1}{a} \end{cases}\Rightarrow b=\frac{1}{2}\left(a^2+\frac{1}{a}\right)$ et $b'=\frac{1}{2}\left(a^2-\frac{1}{a}\right)$.

D'où : $bb'=\frac{1}{4}\left(a^4-\frac{1}{a^2}\right)=-1\Rightarrow a^4+4-\frac{1}{a^2}=0\Rightarrow a^6+4a^2-1=c^3+4c-1=0$.

3.– Comme $a=-x_1-x_2$, $c=a^2\epsilon\mathbb{Q}(x_1,x_2)\leqslant\mathbb{K}=$ le corps de décomposition de P.

Comme X^3+4X-1 n'a pas de racines dans $\mathbb{Q}$ (car s'il y en avait une, ce serait un entier et donc un entier qui divise -1 or ±1 ne sont pas racines), X^3+4X-1 est irréductible sur $\mathbb{Q}$.

Donc $3=[\mathbb{Q}(c):\mathbb{Q}]$ divise $[\mathbb{K}:\mathbb{Q}]$. Comme x_1 est de degré 4 sur $\mathbb{Q}$, on a aussi $4\,|\,[\mathbb{K}:\mathbb{Q}]\Rightarrow 12\,|\,[\mathbb{K}:\mathbb{Q}]$.

4.– Si une racine de P était constructible alors le corps de décomposition $\mathbb{K}$ de P serait inclus dans une extension de degré une puissance de 2 sur $\mathbb{Q}$. C'est impossible car $12\,|\,[\mathbb{K}:\mathbb{Q}]$ n'est pas une puissance de 2.

Exercice 2.

1.– Soit $\mathbb{L}=\mathbb{K}[a]$ et soit P le polynôme minimal de a sur $\mathbb{K}$. Soit $\mathbb{K}\leqslant\mathbb{M}\leqslant\mathbb{L}$.

a) Soit Q le polynôme minimal de a sur $\mathbb{M}$. Alors $Q\epsilon\mathbb{M}[X]\leqslant\mathbb{L}[X]$ divise P (dans $\mathbb{L}[X]$).

Soit $\mathbb{M}'$ le sous-corps de $\mathbb{M}$ engendré par $\mathbb{K}$ et par les coefficients de Q. Alors $Q \epsilon \mathbb{M}'[X]$ et est irréductible donc c'est le polynôme minimal de a sur M'! Donc :

$[\mathbb{L}:\mathbb{M}'] = [\mathbb{M}'(a):\mathbb{M}'] = \deg Q = [\mathbb{L}:\mathbb{M}]$. Donc $[\mathbb{M}':\mathbb{K}] = [\mathbb{M}:\mathbb{K}] \Rightarrow \mathbb{M} = \mathbb{M}'$.

b) Comme il n'y a qu'un nombre fini de facteurs irréductibles (unitaires) de P dans $\mathbb{L}[X]$, le polynôme P n'a qu'un nombre fini de diviseurs unitaires Q dans $\mathbb{L}[X]$. Donc les corps intermédiaires sont en nombre fini.

2.–

a) Montrons que $[\mathbb{L}:\mathbb{K}]$ est algébrique. Soit $x \epsilon \mathbb{L}$. Comme le corps $\mathbb{K}(X)$ a une infinité de sous-corps contenant $\mathbb{K}$ (par exemple pour tout n, $\mathbb{K}(X^{2^{n+1}}) \underset{\neq}{\subset} \mathbb{K}(X^{2^n})$), x est algébrique sur $\mathbb{K}$ (sinon $\mathbb{K}(x) \cong \mathbb{K}(X)$).

Montrons maintenant que $[\mathbb{L}:\mathbb{K}]$ est fini. Sinon, il existe une famille dénombrable infinie $(e_i)_{i \epsilon \mathbb{N}}$ linéairement indépendante sur $\mathbb{K}$. Or la suite croissante de corps :

$$\mathbb{K} \leqslant \mathbb{K}(e_0) \leqslant \mathbb{K}(e_0, e_1) \leqslant \ldots. \leqslant \mathbb{K}(e_0, \ldots., e_n) \leqslant \mathbb{K}(e_{0,\ldots.,} e_{n+1}) \leqslant \ldots.$$

est stationnaire (car il n'y a qu'un nombre fini de corps intermédiaires. Donc il existe N tel que $\mathbb{K}(e_0, \ldots., e_N) = \mathbb{K}(e_0, \ldots., e_n)$ pour tout $n \geqslant N$.

Mais alors $\mathbb{K}(e_i, i \epsilon \mathbb{N}) = \bigcup_n \mathbb{K}(e_0, \ldots., e_n) = \mathbb{K}(e_0, \ldots., e_N)$ est une extension finie. Notons d son degré.

Forcément, $e_{0,\ldots.,} e_d$ sont liés ! D'où la contradiction.

b) Si $\mathbb{K}$ est fini, $\mathbb{L}$. Donc $\mathbb{L}^\times$ est cyclique. Si x engendre $\mathbb{L}^\times$comme groupe , alors a fortiori, $\mathbb{L} = \mathbb{K}(x)$.

c) Si $\mathbb{K}$ est infini, les corps $\mathbb{K}(a + tb)$ ne sont pas deux à deux distincts (il n'y a qu'un nombre fini de corps intermédiaires). Donc il existe $t \neq t'$ dans $\mathbb{K}$ tels que $\mathbb{K}(a + tb) = \mathbb{K}(a + t' b)$. Mais alors $b = \frac{a + tb - (a + t' b)}{t - t'} \epsilon \mathbb{K}(a + tb)$. Donc $\mathbb{K}(a, b) = \mathbb{K}(a + tb)$.

Soient $a_{1,\ldots.,} a_n$ une famille finie telle que $\mathbb{L} = \mathbb{K}(a_{1,\ldots.,} a_n)$. Par exemple il suffit de choisir une base. Alors on montre par récurrence sur $n \epsilon \mathbb{N}$, que $\mathbb{K}(a_{1,\ldots.,} a_n)$ est primitive.

Contre-exemple. L'extension $\mathbb{F}_p(X^p, Y^p) < \mathbb{F}_p(X, Y)$ n'est pas primitive …

Exercice 3.

Le groupe de Galois d'un polynôme de degré 2 est soit $\mathbb{Z}/2\mathbb{Z}$ soit trivial.

Exercice 4.

Soit $P = (X - x_1)(X - x_2)(X - x_3) = X^3 + aX^2 + bX + c$ un polynôme irréductible sur un corps $\mathbb{K}$. On note $\delta = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$ et $\Delta = \delta^2$.

1.– $\mathbb{L}=\mathbb{K}(x_1,x_2,x_3)=\mathbb{K}(x_1,x_2)$ car $x_1+x_2+x_3=-a\epsilon\mathbb{K}$.

De plus x_2 est annulé par $\frac{P(X)}{X-x_1}\epsilon\mathbb{K}(x_1)[X]$ qui est de degré 2. Comme P est irréductible, on a $[\mathbb{K}(x_1):\mathbb{K}]=3$. Donc $[\mathbb{L}:\mathbb{K}]=[\mathbb{K}(x_1,x_2):\mathbb{K}]=\underbrace{[\mathbb{K}(x_1,x_2):\mathbb{K}(x_1)]}_{=1 \text{ ou } 2}[\mathbb{K}(x_1):\mathbb{K}]=3$ ou 6.

2.– Supposons $\mathbb{L}/\mathbb{K}$ séparable. Le groupe de Galois s'identifie à un sous-groupe de $\mathfrak{S}_3$, groupe de permutations des racines de P. Donc $\mathrm{Gal}(\mathbb{L}/\mathbb{K})\cong\mathfrak{S}_3$ ou $\mathbb{Z}/3\mathbb{Z}$.

3.– Si Δ n'est pas un carré alors $\delta\epsilon\mathbb{L}$ est de degré 2 sur $\mathbb{K}$. Donc $2\,|\,[\mathbb{L}:\mathbb{K}]$ et $[\mathbb{L}:\mathbb{K}]=6$.

4.– On a : $\delta=P'(x_1)(x_3-x_2)$ et $x_3+x_2=-a-x_1$.

Donc **si $\mathbb{K}$ est de caractéristique $\neq 2$,** alors $x_3=\frac{1}{2}\left(\frac{\delta}{P'(x_1)}-a-x_1\right)$ et $x_2=-\frac{1}{2}\left(\frac{\delta}{P'(x_1)}+a+x_1\right)$ sont dans $\mathbb{K}(x_1,\delta)$. Donc $\mathbb{L}=\mathbb{K}(x_1,x_2,x_3)=\mathbb{K}(x_1,\delta)$. Donc si Δ est un carré dans $\mathbb{K}$, alors $\delta\epsilon\mathbb{K}$. Donc $\mathbb{L}=\mathbb{K}(x_1)$ et $[\mathbb{L}:\mathbb{K}]=3$.

Contre-exemple en caractéristique 2. Soit $P(X)=X^3+tX+t\epsilon\mathbb{F}_2(t)[X]$. C'est un polynôme irréductible[1] sur $\mathbb{F}_2(t)$, corps des fractions rationnelles en la variable t sur $\mathbb{F}_2$. Lediscriminant est $-4t^3-27t^2=-27t^2=t^2$ (car on est en caractéristique 2) donc $\delta=t$. Notons x_1,x_2,x_3 les 3 racines de P dans une certaine extension du corps $\mathbb{F}_2(t)$: $P(X)=X^3+tX+t=(X-x_1)(X-x_2)(X-x_3)$.

Posons $\alpha=x_1^2x_2+x_2^2x_3+x_3^2x_1$ et $\beta=x_1x_2^2+x_2x_3^2+x_3x_1^2$.

Alors $(X-\alpha)(X-\beta)=X^2+tX+(t^3+t^2)$ est irréductible sur $\mathbb{F}_2(t)$[2].

Donc le corps de décomposition $\mathbb{F}_2(t)(x_1,x_2,x_3)\neq\mathbb{F}_2(t)(x_1)=\mathbb{F}_2(t)(x_1,\delta)$.

Exercice 5.

Soit p un nombre premier. Soit n un entier tel que $\sqrt[p]{n}\notin\mathbb{Q}$.

1.– Le polynôme $P(X)=X^p-n$ n'apas de racines dans $\mathbb{Q}$. Soit Q un facteur irréductible unitaire de P sur $\mathbb{Q}$. Nous allons montrer que Q=P. Notons $x_1,\ldots,x_d$ les racines de Q dans $\mathbb{C}$. Alors $a=x_1\ldots x_d$ est $\pm$ le coefficient constant de Q donc est rationnel.

Or $a^p=(x_1\ldots x_d)^p=x_1^p\ldots x_d^p=n^d$. Si $d<p$ alors d,p sont premiers entre eux donc il existe des entiers u,v tels que $du+pv=1$. Mais alors : $n=n^{du+pv}=a^{pu}n^{pv}\Rightarrow\sqrt[p]{n}=a^un^v\epsilon\mathbb{Q}$ *absurde !*

Donc $d=p$ et $P=Q$ est irréductible sur $\mathbb{Q}$.

2.– Notons $\mathbb{L}$ le corps de décomposition de P sur $\mathbb{Q}$. Alors les racines de P sont $\zeta^i\sqrt[p]{n}$ $0\leqslant i\leqslant p-1$. Donc $\mathbb{L}=\mathbb{Q}\left(\zeta,\sqrt[p]{n}\right)$. On a

$$[\mathbb{L}:\mathbb{Q}]=\underbrace{[\mathbb{L}:\mathbb{Q}(\zeta)]}_{\leqslant p-1}\underbrace{\left[\mathbb{Q}\left(\sqrt[p]{n}\right):\mathbb{Q}\right]}_{=p}=\underbrace{\left[\mathbb{L}:\mathbb{Q}\left(\sqrt[p]{n}\right)\right]}_{\leqslant p}\underbrace{[\mathbb{Q}(\zeta):\mathbb{Q}]}_{=p-1}$$

Donc $[\mathbb{L}:\mathbb{Q}]=p(p-1)$ car p et $p-1$ sont premiers entre eux.

1. irréductible par le critère d'Eisenstein …

2. irréductible car il n'y a pas de racine (pourdes raisons de degrés) …

3.– On en déduit que $P = X^p - n$ est aussi irréductible sur $\mathbb{Q}(\zeta)$. Donc il existe pour tout $i \epsilon \mathbb{Z}/p\mathbb{Z}$, un morphisme de corps $\mathbb{Q}(\zeta) -$ linéaire $\sigma_i \colon \mathbb{L} \to \mathbb{L}, \sqrt[p]{n} \mapsto \zeta^i \sqrt[p]{n}$.

De même, $X^{p-1} + X^{p-2} + \cdots + 1$ est irréductible sur $\mathbb{Q}\left(\sqrt[p]{n}\right)$ et il existe pour tout $j \epsilon (\mathbb{Z}/p\mathbb{Z})^\times$, un morphisme de corps $\mathbb{Q}\left(\sqrt[p]{n}\right) -$ linéaire $\tau_j \colon \mathbb{L} \to \mathbb{L}, \zeta \mapsto \zeta^j$.

Alors le morphisme $\sigma_{i,j} = \sigma_i \circ \tau_j : \mathbb{L} \to \mathbb{L}$, envoie $\sqrt[p]{n}$ sur $\zeta^i \sqrt[p]{n}$ et ζ sur ζ^j.

4.– $H \cong \mathbb{Z}/p\mathbb{Z}$ et $G \cong (\mathbb{Z}/p\mathbb{Z})^\times$ sont cycliques.

5.– Soit $f \in \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$. Alors $f(\zeta) = \zeta^k$ pour un certain k. Donc $f^{-1} \circ s_{i,1} \circ f(\zeta) = f^{-1} \circ \sigma_{i,1}(\zeta^k) = f^{-1}(\zeta^k) = \zeta$. Et $f^{-1} \circ s_{i,1} \circ f$ est un automorphisme de $\mathbb{L}$ qui est $\mathbb{Q}(\zeta) -$ linéaire. Il est donc de la forme $s_{i',1}$ pourun certain $i' \epsilon \mathbb{Z}/p\mathbb{Z}$. Donc $H \trianglelefteq \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$.

6.– Donc $\mathrm{Gal}(L/\mathbb{Q}) = H \rtimes G$ car $H \cap G$ est trivial et les cardinaux sont les mêmes.