Examen du 18/12/2018

Exercice 1. $\Phi(X) = \Phi_5(X)$ le 5ième polynôme cyclotomique. On sait qu'il est irréductible dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$. Il n'est pas irréductible dans $\mathbb{R}[X]$ car les irréductibles dans celui-ci sont de degré ≤ 2. Enfin il n'est bien sûr pas irréductible dans $\mathbb{C}[X]$, dont les irréd sont de degré 1, puisque $\mathbb{C}$ est algébriquement clos.

Exercice 2. Tout diviseur commun de P, Q divise aussi $UP+VQ$, donc est inversible. Ce qui veut dire que P, Q sont premiers entre eux.

Les éléments $2, X \in \mathbb{Z}[X]$ sont premiers entre eux puisqu'ils sont premiers et non associés. S'il existait $U, V \in \mathbb{Z}[X]$ tels que

$$UX + V \cdot 2 = 1$$

En substituant X par 0, on aurait

$2V(0)=1$ avec $V(0)\in\mathbb{Z}$. Impossible.

Exercice 3 Si F était algébriquement clos, le polynôme non constant $P(X)=1+\prod_{\lambda\in F}(X-\lambda)\in F[X]$ admettrait une racine $\lambda_0\in F$. Or $P(\lambda_0)=1$, absurde.

Exercice 4.

4.1. Soit F^c une clôture algébrique de F. Comme F est finie donc algébrique sur $\mathbb{F}_p$, on sait par le cours que F^c est aussi une clôture algébrique de $\mathbb{F}_p$ et est isomorphe à une clôture algébrique $\overline{\mathbb{F}_p}$ donnée: $\varphi: F^c \xrightarrow{\sim} \overline{\mathbb{F}_p}$. On sait par le théorème de structure que

$$\mathbb{F}_{p^n} = \{x\in\overline{\mathbb{F}_p} \mid x^{p^n}=x\}$$

est l'extension de $\mathbb{F}_p$ degré n

contenue dans $\overline{\mathbb{F}_p}$. Cela étant dit, si $r = [F : \mathbb{F}_p]$, alors $\varphi(F)$ est une $\mathbb{F}_p$-extension de $\overline{\mathbb{F}_p}/\mathbb{F}_p$ de degré r, donc $\varphi(F) = \mathbb{F}_{p^r}$.

Comme $r \mid rd$, on a $\mathbb{F}_{p^r} \subseteq \mathbb{F}_{p^{rd}}$

et $$\left[\mathbb{F}_{p^{rd}} : \mathbb{F}_{p^r}\right] = \left[\mathbb{F}_{p^{rd}} : \mathbb{F}_p\right] / \left[\mathbb{F}_{p^r} : \mathbb{F}_p\right]$$
$$= rd/r = d.$$

Par suite $\varphi^{-1}(\mathbb{F}_{p^{rd}})$ est une extension de $\varphi^{-1}(\mathbb{F}_{p^r}) = F$ de degré d.

Noter que la solution qui consiste à identifier F^c à $\overline{\mathbb{F}_p}$ et donc F à $\mathbb{F}_{p^r}$ est recevable.

4.2. On sait que F_d^* est un groupe cyclique d'ordre $d-1$. Il existe $\alpha \in \mathbb{F}_d^*$ tel que

$$F_d^* = \{\alpha^k \mid k \in \mathbb{Z}\} = \{1, \alpha, \ldots, \alpha^{d-2}\}$$

Donc $F_d^* \subseteq F[\alpha]$. Comme $0 \in F[\alpha]$, on a

$$F[\alpha] \subseteq F_d \subseteq F[\alpha],$$ d'où $F_d = F[\alpha]$.

4.3. Le polynôme minimal $Irr(\alpha, F, X) \in F[X]$ est irréductible de degré $[F[\alpha] : F] = [F_d : F] = d$.

Exercice 5

5.1. Le polynôme dérivé $P'(X) \in \mathbb{Z}[X]$ est de degré 2, donc premier à $P(X)$ car ce dernier est irréductible et ne peut pas diviser $P'(X)$, étant de degré 3. Par Bézout dans $\mathbb{Q}[X]$, il existe $U, V \in \mathbb{Q}[X] \subseteq \mathbb{C}[X]$ tels que

$$1 = UP + VP'.$$

Cette égalité est a fortiori vraie dans $\mathbb{C}[X]$ et implique que $P(X)$ et $P'(X)$ n'ont pas de racine commune

dans $\mathbb{C}$. Donc $P(X)$ n'a pas de racine multiple dans $\mathbb{C}$.

5.2. $P(X) = X^3 + a_2X^2 + a_1X + a_0$, $a_i \in \mathbb{Z}$.

Donc $P(x) \xrightarrow[x \to +\infty]{} +\infty$, $P(x) \xrightarrow[x \to -\infty]{} -\infty$

C'est une fonction continue sur $\mathbb{R}$ qui change de signes, elle a donc au moins un zéro dans $\mathbb{R}$. Supposons que ses zéros dans $\mathbb{C}$ sont tous réels.

$$\alpha_0 < \alpha_1 < \alpha_2$$

Alors $P'(x)$ admet un zéro dans $]\alpha_0, \alpha_1[$ et $]\alpha_1, \alpha_2[$. Par conséquent son discriminant est strictement positif. (sinon $P'(x)$ aurait au plus un zéro réel).

5.3. Comme $P(X)$ est irréductible dans $\mathbb{Q}[X]$, $P(X) = \mathrm{Irr}(\alpha_0, \mathbb{Q}, X)$, donc

$[\mathbb{Q}[\alpha_1] : \mathbb{Q}] = \deg P(X) = 3$.

5.4. Donc le corps $E := \mathbb{Q}[\alpha_0]$, on a

$X - \alpha_0 \mid P(X)$, donc

$P(X) = (X - \alpha_0) P_1(X)$, $P_1(X) \in E[X]$
$\deg P_1 = 2$.

Les facteurs irréductibles de $P_1(X)$ dans $E[X]$ sont de degré $\leq \deg P_1 = 2$, ce qui montre 5.4.

5.5 Soient $\alpha_1, \alpha_2 \in \mathbb{C} \setminus \mathbb{R}$ les racines non réelles de $P(X)$. Alors

$K = \mathbb{Q}[\alpha_0, \alpha_1, \alpha_2] \neq \mathbb{Q}[\alpha_0]$

Donc $[K : \mathbb{Q}[\alpha_0]] \geq 2$. Par ailleurs, α_1, α_2 sont les racines de $P_1(X) \in E[X]$ (cf. 5.4), donc $\alpha_1 + \alpha_2 = -b_1 \in E$ si $P_1(X) = X^2 + b_1 X + b_0$. Il suit que $E[\alpha_1, \alpha_2] = E[\alpha_1]$. Donc

$[E(\alpha_1,\alpha_2):E] = [E(\alpha_1):E] \leq 2.$

Par suite $K = E(\alpha_1,\alpha_2]$ est de degré exactement 2 sur E. D'où

$$[K:\mathbb{Q}(\alpha_0)] = [K:E] = 2$$

$$[K:\mathbb{Q}] = [K:\mathbb{Q}(\alpha_0)]\,[\mathbb{Q}(\alpha_0):\mathbb{Q}]$$

$$= 2 \times 3 = 6.$$

5.6. Modulo 2, $F(X) = X^3+X+1 \in \mathbb{F}_2[X]$ est de degré 3 sans racine dans $\mathbb{F}_2 = \{0,1\}$, donc $F(X) \in \mathbb{F}_2[X]$ est irréductible. Donc $F(X) \in \mathbb{Z}[X]$ est irréductible.

Le discriminant de $F'(X) = 3X^2+1$ est négatif. Par 5.2, $F(X)$ possède au plus deux racines réelles.

Mais si $F(X)$ avait deux racines réelles, il aurait une troisième racine réelle, puisque dans $\mathbb{C}$,

la somme de trois racines est égale à

0 (la somme de racines de $X^n + a_{n-1}X^{n-1} + \dots + a_0$ est égale à $-a_{n-1}$). Impossible. Donc X^3+X+1 a exactement une racine réelle.

Les corps de décomposition d'un polynôme étant tous isomorphes entre eux, il suit de 5.5 que tout corps de décomposition de $F(X)$ est de degré 6 sur $\mathbb{Q}$.

Exercice 6

6.1 Soit $\lambda \in \mathbb{C}$ une racine primitive p^r-ième de l'unité, alors $\lambda^{p^{r-1}}$ est une racine primitive p-ième de l'unité et

$$\Phi_p(\lambda^{p^{r-1}}) = 0$$

Donc λ est racine de $\Phi_p(X^{p^{r-1}})$.

Il suit que

$$\Phi_{p^r}(X) = \prod_{\substack{\lambda \in \mathbb{C} \\ \text{racine primitive } p^r\text{ième de } 1}} (X - \lambda)$$

divise $\Phi_p(X^{p^{2-1}})$. Comme

$$\deg \Phi_{p^2}(X) = \varphi(p^2) = p^{2-1}(p-1) = \deg \Phi_p(X^{p^{2-1}}),$$

ces deux polynômes unitaires sont égaux.

6.2. On sait que

$$\Phi_p(X) = \frac{X^p - 1}{X-1} = X^{p-1} + X^{p-2} + \cdots + X + 1,$$

donc par 6.1, on a

$$\Phi_{p^2}(X) = \Phi_p(X^p) = X^{p(p-1)} + X^{p(p-2)} + \cdots + X^p + 1.$$

Exercice 7.

1.a) Par définition $I_1 + I_2$ est l'idéal de A engendré par $I_1 \cup I_2$. Ses éléments s'écrivent sous la forme

$$x_1 + x_2, \text{ avec } x_1 \in I_1, \ x_2 \in I_2.$$

b) $I_1 I_2$ est l'idéal de A engendré par les éléments de la forme

$$x_1 x_2, \quad x_1 \in I_1, \ x_2 \in I_2.$$

Les éléments s'écrivent sous la forme de sommes finies

$$x_{11}x_{21} + x_{12}x_{22} + x_{13}x_{23} + \cdots + x_{1n}x_{2n},$$

avec $x_{1i} \in I_1$, $x_{2i} \in I_2$ et $n \geq 1$.

(7.2) Avec les notations ci-dessus,

$x_{1i}x_{2i} \in I_1$ car $x_{1i} \in I_1$

$\in I_2$ " $x_{2i} \in I_2$

donc $x_{1i}x_{2i} \in I_1 \cap I_2$.

Ce dernier étant un idéal,

$$x_{11}x_{21} + x_{12}x_{22} + \cdots + x_{1n}x_{2n} \in I_1 \cap I_2.$$

Donc $I_1 I_2 \subseteq I_1 \cap I_2$.

7.3. On a $1 \in A$. Par 7.1, il existe $u_1 \in I_1$, $u_2 \in I_2$ tel que.

$$1 = u_1 + u_2$$

7.4 On a $x = xu_1 + xu_2$

avec $xu_1 \in I_1 I_2$ puisque $u_1 \in I_1$
$x \in I_1 \cap I_2 \subset I_2$.

Similairement $xu_2 \in I_1 I_2$. Par 7.2, on a l'inclusion $I_1 I_2 \subseteq I_1 \cap I_2$ et on vient de montrer que $I_1 \cap I_2 \subseteq I_1 I_2$. D'où l'égalité.

7.5. On a

$$a - b = u_1(a-b) + u_2(a-b)$$

Donc $a + u_1(b-a) = b + u_2(a-b)$

Posons $c = a + u_1(b-a)$. Alors

$$c - a = u_1(b-a) \in I_1$$
$$c - b = u_2(a-b) \in I_2.$$

Il suit que $\bar{c}^1 = \bar{a}^1$ et $\bar{c}^2 = \bar{b}^2$.

Cela est exactement la surjectivité de $A \longrightarrow A/I_1 \times A/I_2$.

7.6. Le noyau de l'application ci-dessus est $\{x \in A \mid \bar{x}^1 = 0, \bar{x}^2 = 0\}$
$= \{x \in A \mid x \in I_1, x \in I_2\} = I_1 \cap I_2$.

Par 7.4, $I_1 \cap I_2 = I_1 I_2$. Par le théorème de factorisation des homomorphismes d'anneaux, on obtient un isomorphisme

$$A/I_1 I_2 = A/I_1 \cap I_2 \xrightarrow{\sim} A/I_1 \times A/I_2.$$

7.7. Le théorème de Bézout dit que

$$m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}.$$

On applique 7.6. avec $A = \mathbb{Z}$, $I_1 = n\mathbb{Z}$ et $I_2 = n\mathbb{Z}$, sachant que

$$I_1 I_2 = nm\mathbb{Z}$$

dans ce cas-là

($x_{1i} = m k_{1i}$, $k_{1i} \in \mathbb{Z}$
$x_{2i} = n k_{2i}$ $k_{2i} \in \mathbb{Z}$

$\Rightarrow x_{1i} x_{2i} = mn\, k_{1i} k_{2i} \in mn\mathbb{Z}$

$\Rightarrow x_{11}x_{21} + x_{12}x_{22} + \cdots + x_{1n_2}x_{2n_2} \in mn\mathbb{Z}$).