Corrigé du premier contrôle continu, théorie des corps, 2023

Exercice 1. $\mathbb{Q}(\sqrt{2})$ est de degré 2 sur $\mathbb{Q}$ parce que le polynôme minimal de 2 est X^2-2, irréductible par Eisenstein. $\mathbb{Q}(i,\sqrt{2})$ est de degré au moins 2 sur $\mathbb{Q}(\sqrt{2})$ parce que i n'est pas réel. Elle est de degré au plus 2 parce que i annule le polynôme X^2+1. Donc elle est de degré 2. Par le théorème de la base télescopique, $\mathbb{Q}(\sqrt{2},i)$ est de degré 4 sur $\mathbb{Q}$.

Plus rapide : $\mathbb{Q}(\sqrt[4]{2})$ est de degré 4 sur $\mathbb{Q}$ parce que $P(X)=X^4-2$ est un polynôme unitaire, irréductible par Eisenstein, et s'annule en $\sqrt[4]{2}$, et c'est donc le polynôme minimal de $\sqrt[4]{2}$.

Exercice 2. La preuve se fait par double inclusion. Pour montrer que $\mathbb{Q}(e^{\frac{2i\pi}{k}},e^{\frac{2i\pi}{n}}) \subset \mathbb{Q}(e^{\frac{2i\pi}{m}})$, il suffit de montrer que $e^{\frac{2i\pi}{k}},e^{\frac{2i\pi}{n}} \in \mathbb{Q}(e^{\frac{2i\pi}{m}})$. Or, si $m=uk=vn$, on a $e^{\frac{2i\pi}{k}}=(e^{\frac{2i\pi}{m}})^u$ et $e^{\frac{2i\pi}{n}}=(e^{\frac{2i\pi}{m}})^v$.

Pour montrer que $\mathbb{Q}(e^{\frac{2i\pi}{m}}) \subset \mathbb{Q}(e^{\frac{2i\pi}{k}},e^{\frac{2i\pi}{n}})$, il suffit de montrer que $e^{\frac{2i\pi}{m}} \in \mathbb{Q}(e^{\frac{2i\pi}{k}},e^{\frac{2i\pi}{n}})$. Or, si d est le pgcd de k et n alors d'une part il existe $u,v\in\mathbb{Z}$ tels que $uk+vn=d$, et d'autre part $dm=kn$, ce qui montre que

$$e^{\frac{2i\pi}{m}} = (e^{\frac{2i\pi}{k}})^v\ (e^{\frac{2i\pi}{n}})^u.$$

Exercice 3. On a $\mathbb{Q}\subset K$. Soient $x,y\in K$. Il existe $m,n\in\mathbb{N}^*$ tels que $x\in\mathbb{Q}(\sqrt[n]{2})$ et $y\in\mathbb{Q}(\sqrt[m]{2})$. Mais $\mathbb{Q}(\sqrt[n]{2})\subset\mathbb{Q}(\sqrt[mn]{2})$ et $\mathbb{Q}(\sqrt[m]{2})\subset\mathbb{Q}(\sqrt[mn]{2})$ (parce que $(\sqrt[mn]{2})^m=\sqrt[n]{2}$). Donc $x,y\in\mathbb{Q}(\sqrt[mn]{2})$, et alors $x^{-1},x+y,xy\in\mathbb{Q}(\sqrt[mn]{2})$, ce qui montre que $x^{-1},x+y,xy\in K$. Donc K est un corps.

Supposons par l'absurde que $K/\mathbb{Q}$ est finie, de degré m. Posons $n=m+1$. L'extension $\mathbb{Q}(\sqrt[n]{2})/\mathbb{Q}$ est finie de degré n. En effet, X^n-2 est irréductible par le critère d'Eisenstein etc.. Alors la dimension de K sur $\mathbb{Q}$ est au moins n. Absurde.

Si $x\in K$, x appartient à une extension finie de $\mathbb{Q}$, à savoir l'un des corps $\mathbb{Q}(\sqrt[n]{2})$. Il est donc algébrique sur $\mathbb{Q}$ par le théorème des éléments algébriques.

Exercice 4. Par exemple $r=\frac{9}{4}$. On le trouve comme suit : puisque le carré de $\sqrt{r+\sqrt{5}}$ est du type $a+b\sqrt{5}$ avec $a,b\in\mathbb{Q}$ et b non nul, l'extension $\mathbb{Q}(\sqrt{5})$ est incluse dans $\mathbb{Q}(\sqrt{r+\sqrt{5}})$, donc pour que cette dernière soit de degré 2 sur $\mathbb{Q}$ il faut qu'elle soit égale à $\mathbb{Q}(\sqrt{5})$, c'est-à-dire qu'on ait $\sqrt{r+\sqrt{5}}=a+b\sqrt{5}$, avec $a,b\in\mathbb{Q}$. Il faut juste avoir $2ab=1$ et ensuite $r=a^2+5b^2$. On a choisi $a=1$ et $b=\frac{1}{2}$, mais il y a une infinité de solutions.

Exercice 5. (b) (unicité) Les éléments d'un tel sous-corps vérifient l'équation $x^{p^m}=x$, ils sont donc racines d'un polynôme de degré m et donc il ne peut pas y avoir plus de p^m. S'il y avait deux tels sous-corps distincts à p^m éléments, leur réunion fournirait plus de solutions à cette équation.

(a) Le polynôme $X^{p^m}-X$ est scindé sur K, parce qu'il divise $X^{p^n}-X$ (preuve ci-dessous), il a des racines simples parce que sa dérivée formelle est -1 et il a donc p^m racines dans K. Elles forment un sous-corps (vérification comme dans le cours). Il a p^m éléments.

Montrons que $X^{p^m}-X$ divise $X^{p^n}-X$. Il suffit de montrer que $X^{p^m-1}-1$ divise $X^{p^n-1}-1$. Posons $n=km$. Alors $p^n-1=(p^m)^k-1=(p^m-1)(\sum_{j=0}^{k-1}p^j)$. Donc p^m-1 divise p^n-1. Notons u le quotient. Alors $X^{p^n-1}-1=(X^{p^m-1})^u-1=(X^{p^m-1}-1)(\sum_{j=0}^{u-1}(X^{p^m-1})^j)$. Donc $X^{p^m-1}-1$ divise $X^{p^n-1}-1$.

Deuxième solution. Il y a une autre solution : le groupe $K^\times$ est d'ordre $p^n - 1$. Il est cyclique, et $p^m - 1$ divise $p^n - 1$, il a donc un sous-groupe d'ordre $p^m - 1$, qui est par conséquence l'ensemble de ses éléments qui vérifient $x^{p^n-1} = 1$. En ajoutant 0, on montre qu'on obtient l'ensemble des éléments qui vérifient $x^{p^m} = x$, qui a d'après ce qui précède p^m éléments, et qu'on montre être un corps par la pratique habituelle : il est clair qu'il est stable par produit et passage à l'inverse, quant à la somme on utiliser $(x + y)^{p^m} = x^{p^m} + y^{p^m}$.