Université Rennes 1, Année 2013-2014
Master 1 Math., Algèbre générale de base

Corrigé de l'exercice 3.4, questions 3 et 4

3. (*) Montrer que $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$. *En déduire* $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}]$.

Nous avions déjà montré que $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$, et il ne reste que la deuxième partie de la question à traiter. En introduisant l'extension intermédiaire $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$, on trouve:

$$\begin{aligned}[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] &= [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] \\ &= [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})]\,[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \\ &= 2\,[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})].\end{aligned}$$

Il ne reste qu'à calculer $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})]$. Bien sûr, l'élément $\beta = \sqrt{3}$ est annulé par le polynôme $X^2 - 3$ à coefficients (dans $\mathbb{Q}$ donc) dans $\mathbb{Q}(\sqrt{2})$.

Montrons que ce polynôme est irréductible dans $\mathbb{Q}(\sqrt{2})[X]$. Pour cela, d'après les formules habituelles de résolution des équations de degré 2, il suffit de montrer que le discriminant de $X^2 - 3$ n'est pas un carré dans $\mathbb{Q}(\sqrt{2})$. Le discriminant vaut $\Delta = 12 = 3.2^2$ et c'est un carré dans $\mathbb{Q}(\sqrt{2})$ si et seulement si 3 est un carré dans $\mathbb{Q}(\sqrt{2})$. Supposons donc que 3 est le carré de $a + b\sqrt{2}$ avec $a, b \in \mathbb{Q}$, c'est-à-dire que $a^2 + 2b^2 + 2ab\sqrt{2} = 3$. C'est équivalent au système d'équations $a^2 + 2b^2 = 3$ et $ab = 0$; en utilisant le fait que 2 n'est pas un carré dans $\mathbb{Q}$, on voit que ce système n'a pas de solution.

On a montré que $X^2 - 3$ est irréductible dans $\mathbb{Q}(\sqrt{2})[X]$, donc $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ puis $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = 4$.

4. Trouver le polynôme minimal de $\sqrt{2}+\sqrt{3}$ *sur* $\mathbb{Q}$ *et montrez qu'il est réductible dans* $(\mathbb{Z}/p\mathbb{Z})[X]$ *pour tout* $p \in \mathbb{N}$ *premier. (Indication: utiliser la première question.)*

Posons $\alpha = \sqrt{2}+\sqrt{3}$. On a $\alpha - \sqrt{2} = \sqrt{3}$ donc en élevant au carré:

$$\alpha^2 - 2\sqrt{2}\alpha + 2 = 3.$$

On en déduit que $\alpha^2 - 1 = 2\sqrt{2}\alpha$, puis en élevant au carré $\alpha^4 - 2\alpha^2 + 1 = 8\alpha^2$. Ainsi α est racine du polynôme $P = X^4 - 10X^2 + 1$. Or d'après la question précédente, l'extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}+\sqrt{3})$ est de degré 4 donc le polynôme minimal $f_{\alpha,\mathbb{Q}}$ de α sur $\mathbb{Q}$ est de degré 4. Comme P est divisible par $f_{\alpha,\mathbb{Q}}$, il doit lui être égal.

Montrons maintenant que P est réductible modulo p pour tout p. Si $p = 2$, on a $P = X^4 + 1 = (X+1)^4$ qui est réductible. Dans la suite, on suppose que $p \neq 2$ et on peut alors utiliser la question 1: celle-ci nous dit que dans $\mathbb{F}_p^\times$, soit 2 est un carré, soit 3 est un carré, soit 6 est un carré.

Supposons que 2 est un carré, c'est-à-dire que $2 = a^2$ avec $a \in \mathbb{F}_p$. On doit fabriquer un facteur de P pour montrer que celui-ci n'est pas irréductible. On peut

s'inspirer du calcul que l'on a fait juste au-dessus pour trouver le polynôme minimal de α: on voit qu'à une étape intermédiaire on a obtenu $\alpha^2 - 1 = 2\sqrt{2}\alpha$, c'est-à-dire que le polynôme $X^2 - 2\sqrt{2}X - 1$ annule α. Ce calcul était fait dans $\mathbb{Q}(\alpha)$, mais en fait peut importe que le sous-corps premier soit $\mathbb{Q}$, car on voit bien que dans n'importe quel corps K' qui contient une racine carrée de 2 et une racine carrée de 3, on pourra faire les mêmes calculs avec l'élément $\alpha' = \sqrt{2} + \sqrt{3}$. (Par exemple, on peut prendre pour K' une clôture algébrique de $\mathbb{F}_p$.) Revenant à nos hypothèses, on a $2 = a^2$ dans $\mathbb{F}_p$ et on peut donc penser que $X^2 - 2aX - 1$ sera un diviseur de P. Il ne nous reste qu'à le vérifier en faisant une division euclidienne, et on trouve :

$$X^4 - 10X^2 + 1 = (X^2 - 2aX - 1)(X^2 + 2aX - 1).$$

Supposons maintenant que 3 est un carré: $3 = b^2$ avec $a \in \mathbb{F}_p$. Il est naturel de penser qu'on va deviner un facteur de P en faisant le même calcul que celui fait au départ mais en faisant jouer à $\sqrt{3}$ le rôle que jouait $\sqrt{2}$. Pour cela, on écrit $\alpha - \sqrt{3} = \sqrt{2}$ et on élève au carré pour trouver $\alpha^2 - 2\sqrt{3}\alpha + 3 = 2$. Ainsi le polynôme $X^2 - 2\sqrt{3}X + 1$ annule α. Revenant à $\mathbb{F}_p$ avec $3 = b^2$, on est amené à tester le facteur $X^2 - 2bX + 1$ et on vérifie en effet facilement que:

$$X^4 - 10X^2 + 1 = (X^2 - 2bX + 1)(X^2 + 2bX + 1).$$

D'après la question 1, si dans $\mathbb{F}_p$ ni 2 ni 3 n'est un carré alors 6 est un carré: $6 = c^2$ avec $c \in \mathbb{F}_p$. Ici, l'astuce est de voir qu'en élevant directement au carré l'égalité $\alpha = \sqrt{2} + \sqrt{3}$ on va faire apparaître $\sqrt{6}$ dans le double produit:

$$\alpha^2 = 2 + 3 + 2\sqrt{6}.$$

Ainsi, revenant à $\mathbb{F}_p$ avec $6 = c^2$, on est amené à tester le facteur $X^2 - 5 - 2c$. On trouve:

$$X^4 - 10X^2 + 1 = (X^2 - 5 - 2c)(X^2 - 5 + 2c).$$

On a bien montré que $X^4 - 10X^2 + 1$ est réductible pour tout p.