Université Rennes 1, Année 2012-2013
Master 1 Math., Algèbre générale de base

Exercices sur les extensions de corps, chapitre 1
indications de correction

Exercice 1.8

1) Montrons que X^2+1 ne possède pas de zéro dans $\mathbb{Q}(\sqrt{-2})$. Notons $\alpha=\sqrt{-2}$ et soit $x=r+s\alpha$ avec $r,s\in\mathbb{Q}$ un zéro éventuel. L'équation $x^2+1=0$ s'écrit $r^2-2s^2+1+2rs\alpha=0$. Comme $\{1,\alpha\}$ est une $\mathbb{Q}$-base de $\mathbb{Q}(\alpha)$, ceci est équivalent à $r^2-2s^2+1=0$ et $2rs=0$. Si $r=0$, on trouve $-2s^2+1=0$ qui n'a pas de solution dans $\mathbb{Q}$ puisque 2 n'est pas un carré dans $\mathbb{Q}$. Si $s=0$, on trouve $r^2+1=0$ qui n'a pas de solution dans $\mathbb{Q}$. Ceci termine la démonstration.

2) Montrons que X^2+1 ne possède pas de zéro dans $\mathbb{Q}(\sqrt[4]{-2})$. Notons $\alpha=\sqrt[4]{-2}$; cet élément est racine du polynôme X^4+2 qui est irréductible (comme on le voit par exemple à l'aide du critère d'Eisenstein), donc $\mathbb{Q}(\sqrt[4]{-2})\simeq\mathbb{Q}[X]/(X^4+2)$ dont une $\mathbb{Q}$-base est $\{1,\alpha,\alpha^2,\alpha^3\}$. Soit $x=r+s\alpha+t\alpha^2+u\alpha^3$ avec $r,s,t,u\in\mathbb{Q}$ un zéro éventuel. L'équation $x^2+1=0$ donne :

$$\begin{cases} r^2-2t^2-4su+1=0 & (1)\\ 2rs-4tu=0 & (2)\\ s^2-2u^2+2rt=0 & (3)\\ 2ru+2st=0 & (4)\end{cases}$$

Si $s=u=0$, on trouve $rt=0$ et $r^2-2t^2+1=0$. Comme on l'a vu ci-dessus en montrant que X^2+1 ne possède pas de zéro dans $\mathbb{Q}(\sqrt{-2})$, ces équations n'ont pas de solution.

Si $s=0$ et $u\neq 0$, les équations (2) et (4) donnent $r=t=0$ et alors l'équation (1) n'a pas de solution.

Si $u=0$ et $s\neq 0$, on trouve de même $r=t=0$ et (1) n'a pas de solution.

Il ne reste que les cas où $s\neq 0$ et $u\neq 0$. Utilisant le fait que 2 n'est pas un carré dans $\mathbb{Q}$, l'équation (3) montre que dans ces cas $rt\neq 0$.

Si $s\neq 0, u\neq 0, t\neq 0$ alors (2) et (4) donnent $r/t=2u/s$ et $r/t=-s/u$. Or $2u/s$ et $-s/u$ sont deux nombres rationnels non nuls de signes opposés, donc ils ne peuvent être égaux.

Si $s\neq 0, u\neq 0, r\neq 0$, en écrivant $t/r=(1/2)s/u$ et $t/r=-u/s$ on conclut de même qu'il n'y a pas de solution.

3) Montrons que X^2+1 ne possède pas de zéro dans $\mathbb{Q}(\alpha)$, avec $\alpha^3+\alpha+1=0$. On montre facilement que le polynôme X^3+X+1 n'a pas de racine dans $\mathbb{Q}$ (en utilisant le fait qu'une racine $x=p/q$ vérifie : p divise $a_0=1$ et q divise $a_n=a_3=1$) donc est irréductible dans $\mathbb{Q}[X]$. Alors $\{1,\alpha,\alpha^2\}$ est une $\mathbb{Q}$-base de $\mathbb{Q}(\alpha)$. Maintenant soit $x=r+s\alpha+t\alpha^2$ avec $r,s,t\in\mathbb{Q}$ un zéro éventuel. L'équation $x^2+1=0$ s'écrit :

$$\begin{cases} r^2-2st+1=0 & (1)\\ -t^2+2rs-2st=0 & (2)\\ s^2-t^2+2rt=0 & (3)\end{cases}$$

L'équation (1) donne $2st=r^2+1>0$ et l'équation (2) donne $2rs=t^2+2st=t^2+r^2+1>0$. Ceci montre que r,s,t sont non nuls et tous trois de même signe ; d'ailleurs si (r,s,t) est solution alors $(-r,-s,-t)$ l'est aussi. Supposons par exemple que r,s,t sont >0. Alors l'équation (3) donne

$t^2 = s^2+2rt > s^2$ d'où $t > s$. Alors (3) et (2) donnent $t^2 = s^2+2rt > s^2+2rs = s^2+t^2+2st > t^2$ ce qui est impossible. Si r, s, t sont < 0 on conclut pareil.

Exercice 1.9

Supposons qu'il existe un polynôme $P \in k[X]$ tel que $P(\alpha^2) = 0$. Soit $Q(X) := P(X^2)$. Alors $Q(\alpha) = 0$, et comme α est transcendant on en déduit que $Q = 0$. Il en découle que $P = 0$, donc α^2 est transcendant.

Montrons que $k(\alpha^2) \subset k(\alpha)$ est stricte en montrant que $\alpha \notin k(\alpha^2)$. En effet, s'il existe des polynômes $P, Q \in k[X]$ tels que $\alpha = P(\alpha^2)/Q(\alpha^2)$ avec $Q(\alpha^2) \neq 0$, alors le polynôme $R(X) := XQ(X^2) - P(X^2)$ annule α. Comme α est transcendant, il s'ensuit que $R = 0$. Alors $P(X)/Q(X) = X$, et $\alpha = \alpha^2$, donc $X^2 - X$ annule α, ce qui est impossible.

Exercice 1.10

1. Puisque $18 = 2 \times 3^2$ et $50 = 2 \times 5^2$, on a $\mathbb{Q}(\sqrt{18}, \sqrt{50}) = \mathbb{Q}(\sqrt{2})$. C'est une extension de $\mathbb{Q}$ de degré 2 et dont une base est $\{1, \sqrt{2}\}$.

2. Si on montre que $X^3 + 3X + 3$ est irréductible sur $\mathbb{Q}(\sqrt{2})$, alors $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \alpha)$ est composée de $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ et de $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2})(\alpha)$ qui sont resp. de degré 2 et 3. Alors l'extension composée sera de degré 6, avec pour base $\{1, \sqrt{2}, \alpha, \sqrt{2}\alpha, \alpha^2, \sqrt{2}\alpha^2\}$.

Pour montrer que $X^3 + 3X + 3$ est irréductible, comme il est de degré 3 il suffit de montrer qu'il n'a pas de racine dans $\mathbb{Q}(\sqrt{2})$. On peut le faire par un calcul direct, en posant les équations comme dans l'exercice 1.8. Voici une autre méthode, pour varier les plaisirs : il s'agit d'appliquer le critère d'Eisenstein pour le polynôme $X^3 + 3X + 3$ à coefficients dans l'anneau $\mathbb{Z}[\sqrt{2}]$, relativement au premier $p = 3$. Pour cela on doit montrer que $\mathbb{Z}[\sqrt{2}]$ est factoriel et que 3 est bien l'un de ses irréductibles. Voici les grandes lignes de la preuve.

On montre en fait que $A = \mathbb{Z}[\sqrt{2}]$ est euclidien. Pour cela on s'inspire de ce que l'on a fait en exercices pour $\mathbb{Z}[i]$. Ce qui joue le rôle du conjugué $\overline{a + ib} = a - ib$ est ici $\overline{a + \sqrt{2}b} = a - \sqrt{2}b$, et ce qui joue le rôle de la norme $N(z) = z\overline{z} = a^2 + b^2$ est ici $N(z) = z\overline{z} = (a+\sqrt{2}b)(a-\sqrt{2}b) = a^2 - 2b^2$. On vérifie que la norme $N : A \to \mathbb{Z}$ est multiplicative, et on pose $\delta(z) = |N(z)|$. On montre que pour tout $z \in \mathbb{Q}(\sqrt{2})$, il existe $y \in A$ tel que $\delta(z - y) < 1$. On en déduit que δ est un stathme euclidien pour A.

Il reste à vérifier que 3 est irréductible ; c'est équivalent à dire qu'il est premier, c'est-à-dire que l'idéal (3) est premier, c'est-à-dire que $A/(3)$ est un anneau intègre. Or, utilisant le fait que $A \simeq \mathbb{Z}[X]/(X^2 - 2)$, on a :

$$A/(3) \simeq \mathbb{Z}[X]/(X^2 - 2, 3) \simeq (\mathbb{Z}[X]/(3))/(X^2 - 2) \simeq \mathbb{F}_3[X]/(X^2 - 2).$$

Comme X^2-2 n'a pas de racine dans $\mathbb{F}_3$, il y est irréductible, et l'anneau quotient $\mathbb{F}_3[X]/(X^2-2)$ est intègre. Ceci conclut.

Exercice 1.12

1) Soit $P = X^3 - 2$. Parmi les sous-corps de $\mathbb{C}$, un corps de rupture est $\mathbb{Q}(\sqrt[3]{2})$, et un corps de décomposition est $\mathbb{Q}(\sqrt[3]{2}, j)$ où $j = \exp(2i\pi/3)$ est une racine primitive troisième de l'unité.

Nota bene : même lorsqu'on se restreint à des sous-corps de $\mathbb{C}$, il n'y a pas unicité du corps de rupture. Dans notre exemple P possède trois corps de rupture sous-corps de $\mathbb{C}$, à savoir $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(j\sqrt[3]{2})$ et $\mathbb{Q}(j^2\sqrt[3]{2})$. En revanche, il y a dans $\mathbb{C}$ un unique sous-corps de décomposition, on peut donc dire LE (sous-)corps de décomposition.

2) Soit $P = X^4 + 1$. Parmi les sous-corps de $\mathbb{C}$, un corps de rupture est $\mathbb{Q}(\omega)$ où $\omega = \exp(i\pi/4)$ est une racine primitive de l'unité. Par ailleurs les autres racines de $X^4 + 1$ dans $\mathbb{C}$ sont ω^3, ω^5 et ω^7 : elles appartiennent toutes à $\mathbb{Q}(\omega)$ si bien que P est décomposé sur un corps de rupture. Ceci montre que LE corps de décomposition est $\mathbb{Q}(\omega)$ également. Dans ce cas le sous-corps (de $\mathbb{C}$) de rupture est unique.

Note bene : $X^4 + 1$ est le polynôme cyclotomique Φ_4.

Exercice 1.13

1) C'est une propriété de l'anneau des polynômes en X que $\{1, X, X^2, \dots\}$ est une famille infinie libre, en particulier X n'est racine d'aucun polynôme à coefficients dans k : il est transcendant. Ceci montre que $k \hookrightarrow k(X)$ est transcendante.

2) On a l'inclusion de corps $k \subset k(h) \subset k(X)$. L'extension $k(h) \subset k(X)$ est finie : en effet, l'égalité $h = f(X)/g(X)$ dit que X est racine du polynôme $P \in k(h)[T]$ défini par $P(T) = hg(T) - f(T)$. Ce polynôme (à coefficients dans $k(h)$ en l'indéterminée T) est de degré (en T) égal à $d = \max(m, n)$, donc $k(h) \subset k(X)$ est de degré $\leq d$. Pour montrer que ce degré est exactement égal à d, il suffit de montrer que P est irréductible, car alors ce sera le polynôme minimal de X sur $k(h)$.

Observation 1 : comme l'extension $k \subset k(X)$ est infinie et $k(h) \subset k(X)$ est finie, alors $k \subset k(h)$ est infinie. Ceci implique que h est transcendant sur k, c'est-à-dire que c'est une indéterminée. On va considérer P comme un élément de $k[h][T]$, anneau de polynômes en deux variables h et T.

Observation 2 : il s'agit du lemme de Gauss sur le contenu des polynômes à coefficients dans un anneau *factoriel* A. Ce lemme affirme que le *contenu* $c(P)$ d'un polynôme $P \in A[X]$, qui est le pgcd de ses coefficients, est multiplicatif, c'est-à-dire que $c(PQ) = c(P)c(Q)$, qui est une égalité à lire aux inversibles près (voir lemme numéro 4.2.16 du cours). Un polynôme de contenu égal à 1, c'est-à-dire sont les coefficients sont premiers entre eux (dans leur ensemble), est dit *distingué*.

Avec des deux observations préliminaires, montrons maintenant que P est irréductible. Considérons une factorisation $P = QR$ avec $Q, R \in k(h)[T]$. Notons $m(h)$ le ppcm des dénominateurs des coefficients de Q, R dans $k(h)$. En multipliant par $m(h)$ on obtient $m(h)P = Q'R'$ avec Q', R' polynômes à coefficients dans $k[h]$ et primitifs. On a donc maintenant une égalité entre éléments de $k[h][T]$, anneau des polynômes en T à coefficients dans l'anneau factoriel $A = k[h]$ (polynômes en h). Notons que comme $P(T) = hg(T) - f(T)$ avec f et g premiers entre eux, alors $c(P) = 1$. D'après le lemme de Gauss rappelé plus haut, on a $m(h) = c(m(h)P) = c(Q'R') = c(Q')c(R') = 1$ ce qui montre que $m(h)$ est inversible. On a donc $P = QR$ avec $Q, R \in k[h][T]$ tous deux primitifs. Or $k[h][T] = k[h, T] = k[T][h]$, anneau de polynômes en h à coefficients dans $k[T]$. L'égalité $P = QR$ comme égalité entre polynômes en h montre que (quitte à échanger Q et R au besoin) Q est constant en h et R est de degré 1 en h. Écrivons $Q = q(T)$ et $R = r(T) + hs(T)$. Alors $P = QR$ donne $hg(T) - f(T) = q(T)r(T) + hq(T)s(T)$. Par identification, on trouve $g = qs$ et $f = -qr$. Comme f et g sont premiers entre eux, ceci implique que $q \in k[T]$ est inversible, i.e. $Q = q \in k^*$. On a ainsi montré que P est irréductible.

3) Si F contient strictement k, il contient un élément $h \notin k$. On a alors $k(h) \subset F \subset k(X)$ et dont on déduit $[k(X) : F] \leq [k(X) : k(h)]$ qui est fini d'après la question précédente.