# Commutative Algebra Exam

Padova, 22/01/2016

**Exercise 1.** Let $R$ be an integrally closed domain, $L$ a finite extension of $K = \operatorname{Frac} R$ and $x \in L$. Let $p(X) \in K[X]$ be the minimal (monic) polynomial of $x$ over $K$. Show that $x$ is integral over $R$ if and only if $p \in R[X]$. [Hint: consider the splitting field of $p$.]

**Exercise 2.** Let $k$ be a perfect field of characteristic 2 and $f(X) \in k[X]$ a non-constant separable polynomial. Put $K = k(X)$ and $L = K[Y]/(Y^2 - f)$. Denote by $A$ the integral closure of $k[X]$ in $L$ and let $\alpha = \sqrt{f}$.

a) Is $A$ a finitely generated $k[X]$-module? Is it free?

b) Let $\xi = a + b\alpha \in A$, $\xi \notin k[X]$, with $a, b \in K$. Show that $a^2 + fb^2 \in k[X]$.

c) Assume $a = \frac{u}{w}$, $b = \frac{v}{w}$, with $u, v, w \in k[X]$. Show that if $\xi \in A$ then $w^2$ divides $f'v^2$ (where $f'$ is the derivative of $f$).

d) Show that if $f'$ is not divisible by a (non-constant) square, then $A = k[X][\alpha]$.

e) Show that $f'$ is always a square.

f) If $\deg f \leq 2$, show that $A = k[X][\alpha]$.

g) If $3 \leq \deg f \leq 4$, write $f' = (X - c)^2$, with $c \in k$ and show that $A = k[X][\frac{\alpha - \sqrt{f(c)}}{X - c}]$.

h) Write $f = gf' + r$ in $k[X]$, with $\deg(r) < \deg f'$. Show that $r' = 0$ and $g' = 1$. [Hint: show that $f'' = 0$.]

i) Show that $g$ is a square in $L$.

j) Conclude that $A = k[X]\left[\sqrt{g}\right]$.

**Exercise 3.** Let $R$ be a local noetherian ring with maximal ideal $\mathfrak{m}$. Show that $\dim R \leq n$ if and only if there exist elements $x_1, \ldots, x_n \in \mathfrak{m}$. such that $R/(x_1, \ldots, x_n)$ is artinian.

You may submit your answers in english, french or italian.

# Solutions[1]

**Exercise 1.** By definition, if $p \in R[X]$, its root $\alpha$ is integral over $R$. Conversely, if $\alpha$ is integral over $R$, there is a monic $q(X) \in R[X]$ with $q(\alpha) = 0$. Let $\alpha_1 = \alpha$, $\alpha_2$, ..., $\alpha_n$ be the conjugates of $\alpha$ in the splitting field $M$ of $p$. By definition, $p$ divides $q$ so the $\alpha_i$ are roots of $q$ and therefore integral over $R$. The coefficients of $p$ belong then to the subring $R[\alpha_1, \dots, \alpha_n] \subset M$ and are thus integral over $R$. They also belong to $K$. Since $R$ is integrally closed, we conclude $p \in R[X]$.

**Exercise 2.** Even though $L/K$ is an inseparable extension, since $k[X]$ is a finitely generated $k$-algebra, Noether's normalisation lemma implies that $A$ is a finite $k[X]$-algebra (corollary 4.3.8 in the notes). Since $k[X]$ is a PID, $A$ is a free module of rank $[L : K] = 2$ (see theorem 5.3.14 in the notes).

We are in characteristic 2, so $\xi^2 = (a+b\alpha)^2 = a^2+b^2 f \in K$. Since $\xi \notin K$, its minimal polynomial over $K$ has degree 2, so $T^2 - a^2 - fb^2$ is the minimal polynomial. Since $\xi$ is integral over $k[X]$, we conclude by exercise 1.

From a) we get that $u^2 + fv^2 = pw^2$ for a suitable $p \in k[X]$. Taking derivatives, we get $f'v^2 = p'w^2$.

Let $\xi \in A$. WLOG we may assume $\gcd(u, v, w) = 1$. From b), since $f'$ has no square facors, we get that $q|v$ for every irreducible factor $q$ of $w$. From equation $u^2 + fv^2 = pw^2$ we get that $q|u$ as well and from the assumption $\gcd(u, v, w) = 1$ we conclude $q \in (k[X])^\times$ for every irreducible factor $q$ of $w$. So $w \in (k[X])^\times = k^\times$, hence $\xi \in k[X] + \alpha k[X] = k[X][\alpha]$.

If $f = \sum_{i=0}^{n} a_i X^i$ then, since $2 = 0$ in $k$, setting $m = \left[\frac{n}{2}\right]$, we have $f' = \sum_{j=0}^{m} a_{2j+1} X^{2j}$. Moreover, since $k$ is perfect, $a_{2j+1} = b_j^2$ for a suitable $b_j \in k$. Therefore $f' = \left(\sum_{j=0}^{m} b_j X^j\right)^2$.

If $f = c_2X^2 + c_1X + c_0$ then $f' = c_1 \in k$ is a constant. It follows from c) that $w \in k^\times$, so $A = k[X][\alpha]$.

If $3 \le \deg f \le 4$ and $f' = (X - c)^2$, put $\beta = \frac{\alpha - \sqrt{f(c)}}{X-c}$. Then $g = \beta^2 = \frac{f - f(c)}{(X-c)^2} \in k[X]$, because $c$ is a double root of $f - f(c)$. Now $\deg g \le 2$ and clearly $L = K(\alpha) = K(\beta)$. From f) we conclude that $A = k[X][\beta]$.

Since $f'$ is a square, $f'' = 0$. Differentiating $f = gf' + r$ we get:

$$f' = g'f' + gf'' + r' = g'f' + r' \quad \Longrightarrow \quad r' = (1 - g')f'.$$

But $\deg r' < \deg r < \deg f'$, so $r' = 0$. Since $f$ is separable, $f'$ is not identically zero, so $g' = 1$.

Since $r' = 0$, $r$ is a square in $k[X]$, say $r = s^2$. We already know that $f'$ is a square, so

$$g = \frac{f - s^2}{f'} = \left(\frac{\alpha - s}{\sqrt{f'}}\right)^2.$$

Therefore $g$ has a square root $\beta \in L$ and the same formula shows that $L = K(\beta)$. Moreover $g' = 1$, so we conclude from d) that $A = k[X][\beta]$.

[1] References to the lecture notes are numbered as in the version of 21/01/2016.

**Exercise 3.** If $\dim R = \operatorname{ht} \mathfrak{m} = h$, we know that there exist $x_1, \ldots, x_h \in R$ such that $\mathfrak{m}$ is one of the minimal primes containing $x_1, \ldots, x_h$ (proposition 6.1.23). By the bijection between prime ideals in $\overline{R} = R/(x_1, \ldots, x_h)$ and primes in $R$ containing $(x_1, \ldots, x_h)$, we may say that $\overline{R}$ is a local ring with maximal ideal $\overline{\mathfrak{m}} = \mathfrak{m}/(x_1, \ldots, x_h)$ and that $\overline{\mathfrak{m}}$ is a minimal prime. Hence $\dim \overline{R} = \operatorname{ht} \overline{\mathfrak{m}} = 0$. If $h < n$, we can just add $x_{h+1} = \ldots = x_n = 0$.

Conversely, let $x_1, \ldots, x_n \in \mathfrak{m}$ such that $\overline{R} = R/(x_1, \ldots, x_n)$ is artinian. If there were a prime $\mathfrak{p} \subset R$ such that $(x_1, \ldots, x_n) \subseteq \mathfrak{p} \subsetneq \mathfrak{m}$, in $\overline{R}$ we would have a chain $\mathfrak{p}/(x_1, \ldots, x_n) \subsetneq \mathfrak{m}/(x_1, \ldots, x_n)$, hence $\dim \overline{R} \geq 1$ and so $\overline{R}$ would not be artinian. Therefore, $\mathfrak{m}$ is a minimal prime ideal containing the $x_i$, so $\dim R = \operatorname{ht} \mathfrak{m} \leq n$ by the generalised Principal Ideal Theorem (6.1.19).