EPFL - Printemps 2021	Prof. Z. Patakfalvi
Anneaux et Corps	**Solutions de l'examen final**

The amount of details I write down is to be considered as sufficient to get full points.

Exercice 1. 1. Let k be a field. We consider the following subsets of the matrix ring $\mathrm{Mat}(k,3)$:

$$I = \left\{ \begin{pmatrix} a & 0 & 0 \\ b & 0 & 0 \\ c & 0 & 0 \end{pmatrix} \mid a,b,c \in k \right\}, \quad I = \left\{ \begin{pmatrix} a & a' & 0 \\ b & b' & 0 \\ c & c' & 0 \end{pmatrix} \mid a,b,c,a',b',c' \in k \right\}$$

Clearly they are subgroups of $\mathrm{Mat}(k,3)$ (no justification needed here). There are also left-ideals. This can be checked by an explicit calculation (which is needed) — or we can interpret $\mathrm{Mat}(k,3)$ as the ring $E := \mathrm{End}_k\left(k^{\oplus 3}\right)$ of k-linear endomorphisms of $k^{\oplus 3}$ written in the standard basis (e_1, e_2, e_3), and then $I = \{\phi \in A \mid \phi(e_3) = 0\}$ and $J = \{\phi \in A \mid \phi(e_2) = \phi(e_3) = 0\}$. Left-multiplication corresponds to post-composition, and clearly the defining properties of I and J are preserved by post-composition.
Now $I \cap J = I$, while

$$IJ \ni \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \notin I.$$

2. Let $\xi := \mathrm{ev}_{x=y^2} \colon F[x,y,z] = F[y,z][x] \to F[y,z]$ be the evaluation morphism given by $x \mapsto y^2$. By Exemple 1.4.10, it holds that $\ker \xi = (x - y^2)$. Then we have the sequence of isomorphisms

$$\frac{F[x,y,z]}{(x-y^2, y^3+z^4)} \cong \frac{F[x,y,z]/(x-y^2)}{(\xi(y^3+x^4))} \cong \frac{F[y,z]}{(y^3+z^4)}$$

where the first isomorphism is given by the Quotient en deux temps (Proposition 1.4.41), the second one by the First isomorphism theorem.

Exercice 2. 1. Since E is a field with q elements, the multiplicative group $E^\times = E \setminus \{0\}$ has $q-1$ elements. By Lagrange's theorem in group theory, we obtain that

$$\alpha^{q-1} = 1 \quad \forall \alpha \in E^\times.$$

Thus every element α of $E^\times$ satisfies $\alpha^q = \alpha$. Of course this is also verified if $\alpha = 0$. Thus every element of E is a root of $x^q - x$. It follows that $f(x) := \prod_{\alpha \in E}(x - \alpha)$ divides $x^q - x$. But f and $x^q - x$ have the same degree and are both monic, thus there are equal. In particular $x^q - x$ splits completely in E. If $E' \subseteq E$ is a subfield where $x^q - x$ also splits completely, then by the UFD property of $E[x]$ we would have $x - \alpha \in E'[x]$ for every $\alpha \in E'$, and thus $E' = E$. Hence E is a splitting field of $x^q - x$.

2. Let $E := \{\alpha \in L \mid \alpha^q - \alpha = 0\}$ be the set of roots of $x^q - x$ in L. We claim that E is a subfield. Indeed, for $\alpha, \beta \in E$:

(a) Clearly $0, 1 \in E$. If q is odd then $(-1)^q = -1$ so $(-1)^q - (-1) = 0$. If q is even then $-1 = 1$. Thus $-1 \in E$.

(b) $(\alpha\beta)^q - \alpha\beta = \alpha^q\beta^q - \alpha\beta = \alpha(\beta^q - \beta) = 0$ so $\alpha\beta \in E$.

(c) $(\alpha+\beta)^q - (\alpha+\beta) = \alpha^q + \beta^q - \alpha - \beta = 0$ since binomial coefficients divisible by p are zero in E. Thus $\alpha + \beta \in E$.

(d) $-\alpha = (-1) \cdot \alpha \in E$.

(e) If $\alpha \neq 0$, then from $\alpha^q = \alpha$ we get $\alpha^{q-1} = 1$ and so $\alpha^{-1} = \alpha^{q-2} \in E$.

Since L is a splitting field of $x^q - x$ and $x^q - x = \prod_{\alpha \in E}(x - \alpha)$ by definition of E, we must have $L = E$ by minimality of L. The derivative of $x^q - x$ is -1, so by Corollaire 3.4.12 the polynomial $x^q - x$ has q distinct roots in L. Thus $|L| = q$.

Exercice 3. 1. We have $F(1) = 1$ and $F(\alpha) = \alpha^2 = \alpha + 1$, thus the matrix of F is

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

2. We have $F(1) = 1, F(\beta) = \beta^2$ and $F(\beta^2) = \beta^4 = \beta \cdot \beta^3 = \beta^2 + \beta$, so the matrix of F is

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Exercice 4.
Fixons quelques notations. N'importe quel élément non-nul $0 \neq f \in F[[t]]$ peut s'écrire $f = t^{\nu(f)} u_f$, où $u_f \in F[[t]]^\times$. En effet, si $f = \sum_i a_i t^i$, on mettra en évidence t^j avec $j = \min\{i \mid a_i \neq 0\}$. L'entier $\nu(f)$ est uniquement déterminé : car si $t^a u = t^{a+k} v$ avec $k \geq 0$ et $u, v \in F[[t]]^\times$, on a

$$t^a(u - t^k v) = 0$$

et comme $F[[t]]$ est intègre, on obtient $u = t^k v$, donc $k = 0$.

Notons que f est inversible si et seulement si $\nu(f) = 0$, et que $\nu(fg) = \nu(f) + \nu(g)$.

On prétend que f est irréductible si et seulement si $\nu(f) = 1$. Si f est irréductible, alors f n'est pas inversible, donc $\nu(f) > 0$. Si $\nu(f) \geq 2$, alors $f = t \cdot t^{\nu(f)-1} u_f$ montre que f n'est pas irréductible ; donc $\nu(f) = 1$. Inversément, si $\nu(f) = 1$ et que $f = xy$, on a $\nu(x) + \nu(y) = 1$ et donc l'un de $\nu(x), \nu(y)$ est nul, et ainsi l'un de x, y est inversible.

Puisque t est ainsi irréductible, l'écriture $f = t^{\nu(f)} u_f$ est une décomposition en facteurs irréductibles. Concernant l'unicité, supposons que l'on puisse écrire $f = \prod_i g_i^{a_i}$, où les g_i sont irréductibles. Alors on peut écrire $g_i = t u_i$, où les u_i sont inversibles. On a alors $f = t^{\sum_i a_i} \prod_i a_i$. L'argument qui montre que $\nu(\bullet)$ est bien défini, montre que $\sum_i a_i = \nu(f)$, et il s'ensuit que $\prod_i u_i = u_f$. Ceci prouve l'unicité.

Exercice 5.
We verify that in $\mathbb{F}_3[x]$ one has $2x^2 + 1 = -(x-1)(x+1)$. Let $J_1 = (x-1), J_2 = (x+1)$. Then $J_1 \cap J_2 = J_1 J_2 = (2x^2+1)$, while $J_1 + J_2 = \mathbb{F}_3[x]$ since it contains the invertible element $2 = (x+1) - (x-1)$.

Hence by the Chinese Remainder theorem (Théorème 1.4.50), the map

$$\xi := (\mathrm{ev}_1, \mathrm{ev}_{-1}) \colon A = \mathbb{F}_3[x]/(2x^2+1) \longrightarrow \mathbb{F}_3[x]/(x-1) \times \mathbb{F}_3[x]/(x+1) \cong \mathbb{F}_3 \times \mathbb{F}_3$$

is a ring isomorphism.

1. $\xi(x^3+2) = (1^3+2, (-1)^3+2) = (0, 1)$ so $\xi(x^3+2)$ is not invertible. Hence the class of x^3+2 is not invertible in A.
2. Since ξ is a ring isomorphism we have $A^\times \cong (\mathbb{F}_3 \times \mathbb{F}_3)^\times$. It is easy to see that

$$(\mathbb{F}_3 \times \mathbb{F}_3)^\times = \mathbb{F}_3^\times \times \mathbb{F}_3^\times$$

and $|\mathbb{F}_3^\times| = 2$, so $|A^\times| = 4$.

Exercice 6.
Consider the subgroup $H := \langle (123) \rangle \leq A_4$. Then by the Galois correspondence we get an intermediate extension $K \subset L^H \subset L$ such that $[L : L^H] = |H| = 3$. This implies that

$$[L^H : K] = \frac{[L : K]}{[L : L^H]} = \frac{|A_4|}{|H|} = \frac{12}{3} = 4.$$

If $\alpha \in L^H$ then we can consider α as an element of L and thus $m_{\alpha,K}$ is separable over K, since the extension $K \subset L$ is separable (Proposition 3.6.10). Hence the extension $K \subset L^H$ is separable. It is also finite, thus by the Primitive element theorem (Théorème 3.5.10) there exists $a \in L^H$ such that $L^H = K(a)$.

We have $\deg m_{a,K} = [K(a) : K] = 4$. We claim that $K(a)$ is not a splitting field of $m_{a,K}$. If it was, then by Théorème 3.6.15 the extension $K \subset K(a)$ would be Galois. By the Fundamental theorem (Théorème 3.6.18), we would obtain that H is a normal subgroup of A_4. But it is not, for

$$(12)(34)(123)(12)(34) = (142) \notin A_4.$$

Since $m_{a,K}$ splits over L (Proposition 3.6.10), it contains a splitting field of $m_{a,K}$ over K, say $K \subset E \subset L$. We have $K(a) \subset L$, and equality does not hold since $K(a)$ is not the splitting field of $m_{a,K}$. Therefore

$$3 = [L : K(a)] = [L : E] \underbrace{[E : K(a)]}_{>1}$$

and we deduce that $[L : E] = 1$, which means $L = E$.

Therefore L is the splitting of the polynomial $m_{a,K}$, which has degree 4.