Lior Silberman's Math 412: Supplementary Problem Set on the Rational Canonical Form

We give an alternative construction of a canonical form over a general field F. When F is algebraically closed this reduced to the Jordan canonical form. To start fix a finite-dimensional vector space V and $T \in \mathrm{End}_F(V)$.

1. (Generalized eigenspaces) For monic irreducible $p \in F[x]$ define $V_p = \left\{ \underline{v} \in V \mid \exists k : p(T)^k \underline{v} = \underline{0} \right\}$.
   (a) Show that V_p is a T-invariant subspace of V and that $m_{T \restriction V_p} = p^k$ for some $k \geq 0$, with $k \geq 1$ iff $V_p \neq \{\underline{0}\}$. Conclude that $p^k | m_T$.
   (b) Let $f \in F[x]$. Show that the restriction $f(T) \restriction V_p$ is invertible iff $p \nmid f$.
   (c) Show that if $\{p_i\}_{i=1}^r \subset F[x]$ are distinct monic irreducibles then the sum $\bigoplus_{i=1}^r V_{p_i}$ is direct.
   (d) Let $\{p_i\}_{i=1}^r \subset F[x]$ be the prime factors of $m_T(x)$. Show that $V = \bigoplus_{i=1}^r V_{p_i}$.
   (e) Suppose that $m_T(x) = \prod_{i=1}^r p_i^{k_i}(x)$ is the prime factorization of the minimal polynomial. Show that $V_{p_i} = \mathrm{Ker}\, p_i^{k_i}(T)$ and that $m_{T \restriction V_{p_i}} = p_i^{k_i}$.

We can now concentrate on each V_{p_i}, so from now on we may assume $m_T(x) = p(x)^k$ with p irreducible of degree d.

2. Let $K = F[x]/(p(x))$ (quotient of the ring $F[x]$ by the ideal $pF[x]$).
   (a) Show that K is a field, generated over K by the image of the polynomial $x \in F[x]$ (write β for this image, so that $K = F(\beta)$).
   (b) Let W be an F-vector space and $T \in \mathrm{End}_F(W)$ with minimal polynomial p. Show that W has the structure of a K-vector space where multiplication by elements of F still has the same meaning and such that $\beta \underline{w} = T\underline{w}$.
   Hint: for $f \in F[x]$ set $(f + (p(x)) \cdot \underline{w} = f(T)\underline{w}$. Start by checking that this is well-defined (independent of the choice of f).
   – Recall now that we are working in a vector space V such that $p(T)^k = 0$ for some k.
   (c) Let $W_i = \mathrm{Im}(p(T)^i) \cap \mathrm{Ker}(p(T))$. Show that $\{0\} = W_k \subset \cdots \subset W_0 = \mathrm{Ker}(p(T))$ and that each W_i is a K-subspace of W_0 for the vector space structure of 2(b).

3. (Chains and the basis)
   DEF Let $B \subset V$ be a set of vectors such that $p(T)B \subset B \cup \{\underline{0}\}$. Call B "linearly independent over K" if for any assignment of polynomials $f_{\underline{v}} \in F[x]^{<d}$ (degrees strictly less than that of p) to vectors $\underline{v} \in B$, having $\sum_{\underline{v} \in B} f_{\underline{v}}(T)\underline{v} = \underline{0}$ forces $f_{\underline{v}} = 0$ for each vv.
   (a) Show that the set B is "linearly independent over K" iff $B \cap \mathrm{Ker}(p(T))$ is linearly independent over K in the sense of 2(b).
   (b) Let $B \subset V$ satisfy $p(T)B \subset B \cup \{\underline{0}\}$ and suppose that $B \cap \mathrm{Ker}(p(T))$ is linearly independent over K. Show that $C = \left\{ T^\ell \underline{v} \mid \underline{v} \in B, 0 \leq \ell < d \right\} \subset V$ is linearly independent over F.
   (c) Choose a K-basis $A \subset W_0 = \mathrm{Ker}(p(T))$ subordinate to the filtration by the W_i (that is, $A \cap W_i$ is a basis for W_i for each i) by choosing a K-basis for W_{k-1}, extending it to a basis of W_{k-2} and so on. Write $A = \{\underline{v}_i\}_{i \in I}$ and let k_i be such that $\underline{v}_i$ was chosen in $W_{k_i - 1}$ so that $\underline{v}_i \in \mathrm{Im}(p(T)^{k_i - 1})$. In that case choose $\underline{v}_{i,k} \in V$ such that $p(T)^{k-1}\underline{v}_{i,k} = \underline{v}_i$ and let $\underline{v}_{i,j} = p(T)^{k-j}\underline{v}_{i,k}$ for $1 \leq j \leq k$. Show that $B = \left\{ \underline{v}_{i,j} \mid i \in I, 1 \leq j \leq k_i \right\}$ is "linearly independent over K".
   (d) Let $\underline{v}_{i,j,\ell} = T^\ell \underline{v}_{i,j}$. Show that $C = \left\{ \underline{v}_{i,j,\ell} \mid \underline{v}_{i,j} \in B, 0 \leq \ell < d \right\}$ is an F-basis for V.

(e) Let $p(x) = x^d - \sum_{i=0}^{d-1} a_i x^i$. Show that

$$T\underline{v}_{i,j,\ell} = \begin{cases} \underline{v}_{i,j,\ell+1} & \ell < d-1 \\ \sum_{\ell=0}^{d-1} a_\ell \underline{v}_{i,j,\ell} + \underline{v}_{i,j-1,0} & \ell = d-1,\, j > 1 \\ \sum_{\ell=0}^{d-1} a_\ell \underline{v}_{i,1,\ell} & \ell = d-1,\, j = 1\,. \end{cases}$$

4. (Rational canonical form)
   (a) Show that $\mathrm{Span}_F \left\{ \underline{v}_{i,j,\ell} \mid 1 \leq j \leq k_i,\, 0 \leq \ell < d \right\}$ is T-invariant. Call its span a *block*. Show that the matrix of T on the block depends only on T and k_i,
   (b) Putting together the blocks for distinct p show that any $T \in \mathrm{End}_F(V)$ we can decompose V as the direct sum of blocks for various polynomials. The resulting matrix representation is called the *rational canonical form*.
   (c) Show that in any two such decompositions the set of polynomials and the number of blocks of each size is uniquely determined. Conclude that we have a bijection between similarity classes of matrices in $M_n(F)$ and rational canonical forms.

5. (Conclusions)
   (a) Show that if all the roots of $m_T(x)$ lie in F, the rational canonical form is the Jordan form.
   (b) Let $A, B \in M_n(F)$ be two matrices and suppose that for some field $\bar{F} \supset F$ there is $S \in \mathrm{GL}_n(\bar{F})$ such that $SAS^{-1} = B$. Show that A, B have the same rational canonical form, and conclude that two matrices are similar over an extension field iff they are similar over the ground field.

6. (conjugacy classes in $\mathrm{GL}_n(F)$) Let F be a field, and let $G = \mathrm{GL}_n(F)$.
   (a) Enumerate the conjugacy classes in $\mathrm{GL}_2(\mathbb{F}_p)$. Note that $p = 2$ is special.
   (b) Enumerate the conjugacy classes of $\mathrm{GL}_3(\mathbb{F}_p)$. Which primes require separate treatment?