Artin-Schreier Extensions

(a) We check that $f(x) = x^p - x - a$ is separable over F: its formal derivative is -1, so it must be separable with n distinct roots. It follows that the splitting field K for $f(x)$ is a Galois extension of F. It suffices to find n distinct automorphisms of $\mathrm{Gal}(K/F)$ and determine that this group is cyclic.

Let θ denote a root of $f(x)$. If θ is in F, we will see that the splitting field is F.

First see that $\theta + k$ for $k = 1, \dots, p-1$ are distinct roots of $f(x)$: We have $(\theta+1)^p - (\theta+1) - a = \theta^p + 1^p - \theta - 1 - a = \theta^p - \theta - a = 0$ (Frobenius), by induction it follows the above elements are the p distinct roots as desired. So if $\theta \in F$, then all the roots of $f(x)$ are in F so that the splitting field is F itself. So we consider the case when $\theta \notin F$.

Observe that the map $\sigma \colon K \to K$ which is the identity on F and maps θ to $\theta + 1$ is an automorphism of K fixing F since it is invertible (the two sided inverse is of course the map that fixes F and sends θ to $\theta - 1$) and permutes roots of $f(x)$. By taking powers, we obtain p distinct automorphisms in $\mathrm{Gal}(K/F)$, and it follows that $\mathrm{Gal}(K/F)$ is cyclic of order p.

(b) View $\sigma, \sigma^2, \dots, \sigma^{p-1}, \sigma^p = \mathrm{id}_K$ as characters $K^\times \to K^\times$. It was already shown that characters are linearly independent (here over K) as functions, so that $\mathrm{Tr}\colon \mathrm{id}_K + \sigma + \cdots + \sigma^{p-1}$ is not the zero function on $K^\times$, so there is a nonzero $\theta \in K$ such that $\mathrm{Tr}(\theta) \neq 0$.

(c) Observe that $\sigma \operatorname{Tr}(\theta) = \sigma\theta + \cdots + \sigma^p\theta = \operatorname{Tr}(\theta)$ since $\sigma^p = \mathrm{id}_K$. In particular this shows that Tr maps into F since σ fixes only the elements in F.

Take $\alpha = (1/\operatorname{Tr}(\theta)) \sum_{i=1}^{p-1} (\sum_{j=0}^{i-1} \sigma^j \beta) \sigma^i \theta$. We have

$$\sigma\alpha = \sigma \left[\frac{1}{\operatorname{Tr}(\theta)} \sum_{i=1}^{p-1} \left(\sum_{j=0}^{i-1} \sigma^j \beta \right) \sigma^i \theta \right] = \frac{1}{\operatorname{Tr}(\theta)} \sum_{i=1}^{p-1} \left(\sum_{j=0}^{i-1} \sigma^{j+1} \beta \right) \sigma^{i+1} \theta,$$

so that

$$\begin{aligned}
\alpha - \sigma\alpha &= \left[\frac{1}{\operatorname{Tr}(\theta)} \sum_{i=1}^{p-1} \left(\sum_{j=0}^{i-1} \sigma^j \beta \right) \sigma^i \theta \right] - \left[\frac{1}{\operatorname{Tr}(\theta)} \sum_{i=1}^{p-1} \left(\sum_{j=0}^{i-1} \sigma^{j+1} \beta \right) \sigma^{i+1} \theta \right] \\
&= \frac{1}{\operatorname{Tr}(\theta)} \big[\beta\sigma\theta + (\beta + \sigma\beta)\sigma^2\theta + \cdots + (\beta + \sigma\beta + \cdots + \sigma^{p-2}\beta)\sigma^{p-1}\theta \\
&\qquad - (\sigma\beta)\sigma^2\theta - \cdots - (\sigma\beta + \sigma^2\beta + \cdots + \sigma^{p-2}\beta)\sigma^{p-1}\theta - (\sigma\beta + \sigma^2\beta + \cdots + \sigma^{p-1}\beta)\theta \big] \\
&= (\beta \operatorname{Tr}(\theta)) / \operatorname{Tr}(\theta) = \beta
\end{aligned}$$

since $-(\sigma\beta + \sigma^2\beta + \cdots + \sigma^{p-1}\beta) = \beta$ by assumption.

(d) Let σ generate $\mathrm{Gal}(K/F)$. We have that $\operatorname{Tr}(-1) = -1 + \cdots + -1 = -p = 0$ since σ fixes F. Then by applying part (c) we have that $-1 = \alpha - \sigma\alpha$ for some $\alpha \in K$; in particular this α could not be in F since σ fixes F. It follows that $\sigma\alpha = \alpha + 1$. By applying σ iteratively to α we obtain p distinct elements of K,

$\alpha + k$ for $k = 0, \ldots, p-1$. Then consider $g(x) = \prod_{k=0}^{p-1}(x - (\alpha + k))$, which is in $F[x]$ since σ (extended to a map on $F[x]$) fixes $g(x)$ as it cycles the roots $\alpha + k$. (The constant term is $\prod_{k=0}^{p-1}(\alpha + k) \in F$).

From part (a), we saw that if θ was a root of $f(x) = x^p - x - a$ for some given $a \in F$, that $\theta + k$ for $k = 0, \ldots, p-1$ form the p distinct roots of $f(x)$. It follows that $\prod_{k=0}^{p-1}(x - (\theta + k)) = x^p - x - a$, so that $a = \prod_{k=0}^{p-1}(\theta + k)$. It follows then that $g(x) = \prod_{k=0}^{p-1}(x - (\alpha + k))$ is equal to $x^p - x - \prod_{k=0}^{p-1}(\alpha + k)$ so that $K = F(\alpha, \ldots, \alpha + p - 1)$ is the splitting field of $g(x) = x^p - x - \prod_{k=0}^{p-1}(\alpha + k)$ as desired.

Direct Limits

(a) A diagram of shape I is a functor $F\colon I \to \mathcal{C}$, and for each $i \in I$ let $F(i) = X_i \in \mathcal{C}$ and let $F(i \leq j) = f_{i,j}\colon X_i \to X_j$ such that $f_{i,i} = \mathrm{id}_{X_i}$, if $i \leq j \leq k$ then $f_{j,k} \circ f_{i,j} = f_{i,k}$, and for any $a, b \in I$ there exists $u \in I$ such that $a \leq u$ and $b \leq u$ so that there exists $f_{a,u}, f_{b,u}$.

The direct limit is a colimit of this diagram; that is, it is an object L with maps $g_i\colon X_i \to L$ such that for any map $f_{i,j}\colon X_i \to X_j$ we have $g_i = g_j f_{i,j}$, and for any other object N with maps $n_i\colon X_i \to N$ such that for any map $f_{i,j}\colon X_i \to X_j$ we have $n_i = n_j f_{i,j}$, there exists a unique morphism $h\colon L \to N$ such that $hg_i = n_i$ for all $i \in I$. This is summarized in the commuting diagram below:

$$\begin{tikzcd}
X_i \arrow[rr, "f_{i,j}"] \arrow[dr, "g_i"] \arrow[ddr, bend right, "n_i"'] & & X_j \arrow[dl, "g_j"'] \arrow[ddl, bend left, "n_j"] \\
& L \arrow[d, dashed, "h"] & \\
& N &
\end{tikzcd}$$

(b) Let the set L be given by the set of equivalence classes of $(\sqcup_{i \in I} X_i)/\sim$ where $x_i \in X_i \sim x_j \in X_j$ if there exists $u \in I$ with $i \leq u, j \leq u$ and $f_{i,u}x_i = f_{j,u}x_j$.

We should check that $\sim$ is an equivalence relation. Reflexivity is clear since there does exist u such that $i \leq u$ and so $f_{i,u}x_i = f_{i,u}x_i$. Symmetry is also clear since equality is symmetric. Transitivity requires a small step: Suppose $x_i \sim x_j$ and $x_j \sim x_k$ so that there exists u_1 with $i \leq u_1, j \leq u_1$ and $f_{i,u_1}x_i = f_{j,u_1}x_j$ and there exists u_2 with $f_{j,u_2}x_j = f_{k,u_2}x_k$. There exists u_3 with $u_1 \leq u_3, u_2 \leq u_3$, from which it follows that $i \leq u_3, k \leq u_3$ and

$$f_{i,u_3}x_i = f_{u_1,u_3}f_{i,u_1}x_i = f_{u_1,u_3}f_{j,u_1}x_j = f_{j,u_3}x_j = f_{u_2,u_3}f_{j,u_2}x_j = f_{u_2,u_3}f_{k,u_2}x_k = f_{k,u_3}x_k.$$

Thus $x_i \sim x_k$ as desired and so $\sim$ is an equivalence relation.

We show that L with maps $g_i\colon X_i \to L$ given by $g_i x_i = [x_i]$ for all $i \in I$ is the direct limit of the diagram F of shape I in the category of sets.

First we check that the maps g_i for all $i \in I$ satisfy the desired commuting property. For $i, j \in I$ with $i \leq j$ we have $g_i = g_j f_{i,j}$: for any $x_i \in X_i$ with $i \leq j$ we show that $g_i x_i = [x_i] = [f_{i,j}x_i] = g_j f_{i,j} x_i$. There exists a $u \in I$ with $j \leq i$ so that also $i \leq u$ and $f_{i,u}x_i = f_{j,u}f_{i,j}x_i$ since $f_{j,u}f_{i,j} = f_{i,u}$. Hence $x_i \sim f_{i,j}x_i$ so that $g_ix_i = g_jf_{i,j}x_i$, and it follows that $g_i = g_jf_{i,j}$ for any $i, j \in I$ with $i \leq j$.

Now suppose that there is an object N with maps $n_i\colon X_i \to N$ such that for $i, j \in I$ with $i \leq j$ we have $n_i = n_jf_{i,j}$. We show that there is a unique map $h\colon L \to N$ such that for all $i \in I$ we have $n_i = hg_i$. Define h by $h[x] = n_kx$, where $i \in I$ is the unique k with $x \in X_k$.

We check that h is well defined first: Let $x_i \sim x_j$ with $x_i \in X_i, x_j \in X_j$, so that there exists $u \in I$ with $i \leq u, j \leq u$ and $f_{i,u}x_i = f_{j,u}x_j$. But $n_i = n_uf_{i,u}$ and $n_j = n_uf_{j,u}$ so that from $f_{i,u}x_i = f_{j,u}x_j$ we have $n_uf_{i,u}x_i = n_ix_i = h[x_i] = h[x_j] = n_jx_i = n_uf_{j,u}x_j$. It follows h is well defined.

The map h defined above also has the desired commuting property, that for all $i \in I$ we have $hg_i = n_i$: for $x_i \in X_i$, $hg_ix_i = h[x_i] = n_ix_i$. The map h is also unique by construction: If there was another (well defined) map h' which could be used in place of h, then for any $[x] \in L$ we have $h'[x] = h'g_ix = n_ix = h[x]$ for some $i \in I$ ($i \in I$ such that $x \in X_i$). Then $h' = h$, so that h is unique. It follows that L satisfies the universal property for being the direct limit of the diagram of shape I in the category of sets.

(c) The direct limit of the groups $\mathbb{Z}/n\mathbb{Z}$ in the category of groups is given by some kind of amalgamated free product of the groups $\mathbb{Z}/i\mathbb{Z}$ for $i \in I$; we will see that this group is just the multiplicative group of (all) roots of unity.

At the expense of taking up more space we use the multiplicative cyclic groups $\mu_n = \{\exp(2\pi ia/n) \mid a \in \mathbb{Z}\} \cong \mathbb{Z}/n\mathbb{Z}$ with maps $f_{n,m}\colon \mu_n \to \mu_m$ given by sending $\exp(2\pi ia/n)$ to $\exp(2\pi i(am/n)/m)$ whenever n divides m. To me it is more clear this way.

Consider the group $L = (*_{i\in I}\mu_n)/N$ where N is the normal closure of the set

$$\bigcup_{n,m\in I} \{\exp(2\pi ia/n)\exp(2\pi i(-b)/m) \mid a, b \in \mathbb{Z} \text{ and } na = mb \in \mathbb{Z}/(nm)\mathbb{Z}\}.$$

This is natural since if $nm \mid (na - mb)$ then $\exp(2\pi ia/n)\exp(2\pi i(-b)/m) = \exp(2\pi i(na - mb)/nm)$ is 1 over $\mathbb{C}$. I will suppress the use of brackets for denoting equivalence classes in the quotient group for this reason. I will also use the multiplication given in $\mathbb{C}$ to reduce words in this group to single elements since the same formula holds due to the construction of N. Observe also that L is Abelian since the product of any two elements $\exp(2\pi ia/n)\exp(2\pi ib/m)$ can be promoted to a product of elements in μ_{nm}, which is Abelian.

We check that L satisfies the universal property for being the direct limit: Let the maps $g_i\colon \mu_i \to L$ be given by the usual inclusion: $\exp(2\pi ia/i) \mapsto \exp(2\pi ia/i)$ and note that they commute with the maps $f_{n,m}$ in the right way since $\exp(2\pi ia/i) = \exp(2\pi i(ja/i)/j)$ in L due to the construction of N.

Let M with maps m_i be any other cocone of our diagram of μ_i for $i \in I$. The map $h\colon L \to M$ is the map taking

$$\prod_{k=1}^{K} \exp\left(2\pi i\frac{a_k}{n_k}\right) = \exp\left(2\pi i\frac{\sum_{k=1}^{K} a_k\frac{\operatorname{lcm}(n_1,\ldots,n_K)}{n_k}}{\operatorname{lcm}(n_1,\ldots,n_K)}\right)$$

to $m_{\operatorname{lcm}(n_1,\ldots,n_K)}\left(\sum_{k=1}^{K} a_k\frac{\operatorname{lcm}(n_1,\ldots,n_K)}{n_k}\right)$. (Any well definedness checks would also work out since the m_i also commute with the $f_{i,j}$ in the right way when $i \mid j$.) This map commutes correctly with the g_i and m_i:

for some fixed $i \in I$ with $\exp(2\pi ia/i) \in \mu_i$ we have that $hg_i \exp(2\pi ia/i) = m_i \exp(2\pi ia/i)$ as expected. By construction the map is unique (Any other map $h' \colon L \to M$ must agree with h everywhere due to the commuting relation h' must satisfy: $h' \exp(2\pi ia/i) = h' g_i \exp(2\pi ia/i) = m_i \exp(2\pi ia/i) = h \exp(2\pi ia/i)$.)

It follows that L is the direct limit of the groups $\mathbb{Z}/n\mathbb{Z}$ with maps $f_{i,j}$ whenever $i \mid j$ up to isomorphism. [The group L may be viewed as the multiplicative group of roots of unity given by $\{\exp(2\pi ia/n) \mid a, n \in \mathbb{Z}\}$ contained in $S^1 \subset \mathbb{C}$ where the product is the usual one taken in $\mathbb{C}$.]

Using Tensor Products in Linear Algebra

(a) A natural map φ from $V^* \otimes_F W \to \mathrm{Hom}_F(V, W)$ is the map taking $\sum_{i=1}^N c_i f_i \otimes w_i$ to $\sum_{i=1}^N c_i f_i(\cdot) w_i$ and note that because $f \colon V \to F$ is linear, $\sum_{i=1}^N c_i f_i(\cdot) w_i \colon V \to W$ is also linear so that it is an element of $\mathrm{Hom}_F(V, W)$. We show that the assignment is an isomorphism when W has finite dimension by checking it is linear, injective, and surjective.

The above assignment is linear by construction: $\varphi[A \sum_{i=1}^N c_i f_i \otimes w_i + B \sum_{j=1}^M d_j g_j \otimes v_j] = A \sum_{i=1}^N c_i f_i(\cdot) w_i + B \sum_{j=1}^M d_j g_j(\cdot) v_j = A\varphi[\sum_{i=1}^N c_i f_i \otimes w_i] + B\varphi[\sum_{j=1}^M d_j g_j \otimes v_j]$.

The map φ is injective as it has trivial kernel. Let $\{w_i\}_{i=1}^N$ be a basis for W. Suppose $\varphi[\sum_{k=1}^K c_k f_k \otimes v_k] = \sum_{k=1}^K c_k f_k(\cdot) v_k = 0$, with $v_k = \sum_{i=1}^N d_{ki} w_i \in W$. We first rewrite $\sum_{k=1}^K c_k f_k \otimes v_k$ as $\sum_{i=1}^N (\sum_{k=1}^K d_{ki} c_k f_k) \otimes w_i$ so that $\sum_{i=1}^N (\sum_{k=1}^K d_{ki} c_k f_k(\cdot)) w_i = 0$ as a linear transformation $V \to W$. It follows by the linear indepedence of the w_i that for each $1 \le i \le N$, $(\sum_{k=1}^K d_{ki} c_k f_k(\cdot)) = 0$ as elements of V^*. It follows that $\sum_{k=1}^K c_k f_k \otimes v_k = \sum_{i=1}^N (\sum_{k=1}^K d_{ki} c_k f_k) \otimes w_i = 0 \in V^* \otimes_F W$.

The map φ is surjective. Given any linear transformation $T \colon V \to W$ and fixing a basis $\{w_i\}_{i=1}^N$ for W, we find a preimage. Observe that $\pi_i \circ T$ for $1 \le i \le N$ where π_i is the projection onto the i-th component (it extracts the i-th coefficient in the expansion of $w \in W$ as a linear combination of basis vectors) is a linear functional in V^*. Furthermore, observe that $T = \sum_{i=1}^N (\pi_i \circ T)(\cdot) w_i$ since the w_i form a basis for W. It follows that $\sum_{i=1}^N (\pi_i \circ T) \otimes w_i$ is a preimage for T under φ.

It follows that φ is an isomorphism of $V^* \otimes_F W$ with $\mathrm{Hom}_F(V, W)$.

(b) For a basis element e_k, we have $Ae_k = \sum_{i=1}^n a_{ik} e_i = \sum_{i=1}^n a_{ik} e_k^*(e_k) e_i$ (the k-th column of A). By linearity, it follows that for any $v \in V$ with $v = \sum_{k=1}^n c_k v_k$,

$$Av = \sum_{k=1}^n c_k A e_k = \sum_{k=1}^n c_k \left(\sum_{i=1}^n a_{ik} e_k^*(e_k) e_i \right) = \sum_{1 \le i,k \le n} a_{ik} e_k^*(c_k e_k) e_i = \sum_{1 \le i,k \le n} a_{ik} e_k^*(v) e_i$$

since $e_k^*(e_i) = \delta_{ki}$ (1 if $i = k$ and 0 otherwise). It follows that

$$A = \sum_{1 \le i,k \le n} a_{ik} e_k^*(\cdot) e_i = \varphi \left[\sum_{1 \le i,k \le n} a_{ik} (e_k^* \otimes e_i) \right]$$

so that under some fixed bases $\{e_i\}, \{e_i^*\}$ for V, V^* respectively, we have $\varphi^{-1} T = \sum_{1 \le i,k \le n} a_{ik} (e_k^* \otimes e_i)$. If we change the bases to a different set of bases, the matrix A for T becomes another matrix A' and we should expect that applying the right change of base matrices to $\{e_i\}, \{e_i^*\}$, we find that the preimage $\sum_{1\leq i,k\leq n} a_{ik}(e_k^* \otimes e_i)$ changes in a way that the coefficients a_{ik} become the entries of the new matrix A'.

(c) Define $\mathrm{Tr}\colon \mathrm{Hom}_F(V,V) \to F$ by $\mathrm{Tr} = \Phi\varphi^{-1}$ where $\Phi\colon V^* \otimes_F V \to F$ is the linear map