Factorization in Artin-Schreier Extenesions and Kummer Extensions

Artin- Schreier Extensions

Let k be a field of char $= p$. Let $0 \neq x \in k$ and consider

$$f(y) = y^p - y - x \in k[y].$$

A good case to have in mind is $k = \mathbb{F}_p(x)$ and so $f(x) \in \mathbb{F}_p(x)[y]$.

Let $\beta \in k$ be a root of $f(y)$.

Observe that $\forall a \in \mathbb{F}_p \subseteq k$,

$$\begin{aligned} f(\beta + a) &= (\beta+a)^p - (\beta+a) - x \\ &= \beta^p - \beta + \underbrace{a^p - a}_{=0} - x \\ &= f(\beta) \\ &= 0. \end{aligned}$$

Thus, the roots of $f(y)$ are precisely $\{\beta + a \mid a \in \mathbb{F}_p\}$.

Definition

The extension $k(\beta)/k$ is called an Artin-Schreier extension.

Now to the rings

Consider now a D.D $A \subseteq k$ with $k = \operatorname{Frac} A$. Assume $x \in A$ and so β is integral over A and so the extension $A[\beta] \cong A[y]/_{\langle f(y) \rangle}$ is integral over A. Since $f'(y) = -1$, $f'(\beta)$ is not contained in any max ideal of $A[\beta]$. From a previous unit we deduce that $A[\beta]_{\mathcal{M}}$ is a PID for all $\mathcal{M} \in \operatorname{Max} A[\beta]$.

Further, $\mathcal{M}$ is unramified over A. Thus, $A[\beta]/A$ is unramified. Since being integrally closed is a local property, we deduce that $A[\beta]$ is integrally closed, and so $A[\beta]$ is the integral closure of A in $k(\beta)$.

$$
\begin{tikzcd}[column sep=small]
\langle x, y-\beta \rangle \arrow[dr, dash, "{\substack{e=1\\ f=1}}"'] & & \langle x, y-\beta-(p-1) \rangle \arrow[dl, dash, "{\substack{e=1\\ f=1}}"] \\
& \langle x \rangle \arrow[u, phantom, "p"] &
\end{tikzcd}
\qquad
\begin{tikzcd}
B = \mathbb{F}_p[x, \beta] \arrow[d, dash] \\
A = \mathbb{F}_p[x]
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathbb{F}_p(x)[y] \big/ \langle y^p - y - x \rangle \cong \mathbb{F}_p(x)(\beta) \arrow[d, dash] \\
k = \mathbb{F}_p(x)
\end{tikzcd}
$$

Kummer Extensions

Let $k = \mathbb{F}_q(x)$ with $q = p^m$, p prime. Let

$$f(y) = y^n - a(x) \in (\mathbb{F}_q[x])[y]$$

be an irreducible polynomial.

Let $\alpha \in \overline{\mathbb{F}_q(x)}$ be a root of $f(y)$. The extension $L = \mathbb{F}_q(x)(\alpha) / \mathbb{F}_q(x)$ is called a Kummer extension.

Let $A = \mathbb{F}_q[x]$. Then, Then, $\mathbb{F}_q[x][\alpha]$ is integral over $\mathbb{F}_q[x]$. By a result we proved,

$$\mathbb{F}_q[x][\alpha] \cong \mathbb{F}_q[x,y] / \langle y^n - a(x) \rangle \text{ is integrally closed} \iff Z_{y^n - a(x)}\left(\overline{\mathbb{F}_q(x)}\right) \text{ is non-singular}$$

$\frac{\partial}{\partial y}(y^n - a(x)) = ny^{n-1}$ and $\frac{\partial}{\partial x}(y^n - a(x)) = -a'(x)$. Thus assuming $\gcd(n,p) = 1$, the curve is non-singular $\iff$ $a(x)$ is square-free.

So, assuming $\gcd(n,p)=1$ and $a(x)$ is square-free we get that $\mathbb{F}_q[x][\alpha]$ is the integral closure of $\mathbb{F}_q[x]$ in $\mathbb{F}_q(x)(\alpha)$. Since $\dim \mathbb{F}_q[x]=1$ and $\mathbb{F}_q[x][\alpha]$ algebraic over $\mathbb{F}_q[x]$, $\dim \mathbb{F}_q[x][\alpha]=1$. As $\mathbb{F}_q[x][\alpha]$ is a f.g $\mathbb{F}_q[x]$ module, and $\mathbb{F}_q[x]$ noetherian, $\mathbb{F}_q[x][\alpha]$ is a D.D.

Write $a(x)=c\cdot\prod_{i=1}^{r}(x-a_i)$ with $a_i\neq a_j$ for $i\neq j$. Consider a maximal ideal $(x-b)\mathbb{F}_q[x]$. How does $(x-b)\mathbb{F}_q[x][\alpha]$ factors? To compute this factorization consider the reduction

$$\bar{f}(y)=y^n-a(b)=y^n-c\cdot\prod_{i=1}^{r}(b-a_i)\in\left(\mathbb{F}_q[x]/\langle x-b\rangle\right)[y]\cong\mathbb{F}_q[y]$$

If $b=a_i$ for some $i\in[r]$ then $\bar{f}(y)=y^n$ and so $\langle x-b\rangle\mathbb{F}_q[x][\alpha]=\langle x-b,y\rangle^n$. otherwise $y^n-a(b)$ has n distinct roots (eg. since the derivative of the reduction is $ny^{n-1}\neq 0$ $\forall y\neq 0$).

Hence, if $\zeta \in \overline{\mathbb{F}_q}$ is an n^{th} root of unity, then $y^n - a(b) = \prod_{i=0}^{n-1} (y - \zeta^i d)$ where $d = d(b) \in \overline{\mathbb{F}_q}$ is s.t. $d^n = a(b)$. Hence, in this case, the ideal $\langle x-b \rangle \mathbb{F}_q[x][\alpha]$ "splits" to n distinct maximal ideals.

$$\begin{tikzcd}[column sep=small] \langle x-b,\, y-\zeta^0 d(b)\rangle \arrow[dr, dash, "{e=1,\ f=1}"'] & \cdots & \langle x-b,\, y-\zeta^{n-1} d(b)\rangle \arrow[dl, dash, "{e=1,\ f=1}"] \\ & \langle x-b\rangle \arrow[u, phantom, "n"] & \end{tikzcd}$$

$\forall\, b \notin \{a_1, \dots, a_r\}$

$$\begin{tikzcd} \langle x-a_i,\, y\rangle \arrow[d, dash, "{e=n,\ f=1}"] \\ \langle x-a_i\rangle \end{tikzcd}$$

$i = 1, \dots, r$

This is the i.c assuming $\gcd(n,p)=1$ and $a(x)$ is square-free

$$\begin{tikzcd} \mathbb{F}_q(x)[\alpha] \arrow[d, dash] & \mathbb{F}_q(x)[y] / \langle y^n - a(x)\rangle \cong \mathbb{F}_q(x)(\alpha) \arrow[d, dash] \\ \mathbb{F}_q[x] & \mathbb{F}_q(x) \end{tikzcd}$$