KNR Lecture #5

Dickson Invariants (following §8.1 of Benson)

$\mathbb{F}_q$ finite field, E v.s./$\mathbb{F}_q$ of dim $n<\infty$. K = ext. field of $\mathbb{F}_q$ (which when necessary we take to be infinite)
$V = E\otimes_{\mathbb{F}_q} K$,. $G = GL_{\mathbb{F}_q}(E)$; G acts on E $\mathbb{F}_q$-linearly, so K-linearly on V, so on $K[V]$ as K-alg auts, and on $K(V)$ by field auts fixing K.

<u>Theorem</u> (DICKSON) $K[V]^G$ is a polynomial ring (of dimension n over K).

<u>Remark:</u> We will obtain generators explicitly later.

Proof, a rather "upside down" one. Let $c_0,\dots,c_{n-1}$ be n indeterminates$/K$. They will turn out to be the desired invariants. When convenient c_j will be assumed to be homogeneous of degree $q^n - q^j$. Set $L_0 := K(c_0,\dots,c_{n-1})$.

$$f(X) := X^{q^n} - c_{n-1}X^{q^{n-1}} + c_{n-2}X^{q^{n-2}} \pm \dots \pm (-1)^i c_{n-i} X^{q^{n-i}} \pm \dots + (-1)^n c_0 X^{q^0}$$

This is separable: $f'(X) = (-1)^n c_0$. Let L = Splitting field over L_0 of $f(X)$.
Since $f(X)$ involves only powers of X of degree that are powers of q, the roots of $f(X)$ form an $\mathbb{F}_q$-vector subspace — call it W — of L. $|W| = q^n$ $(=\deg f)$ so $\dim_{\mathbb{F}_q} W = n$.

Think of E as W^*, so that $W = E^*$. We have:

$$\begin{tikzcd} K[V] \arrow[r, hook, "\varphi"] & K[\text{the roots of } f(X)] \arrow[r, phantom, "\subset"] & L \\ & K[c_0,\dots,c_{n-1}] \arrow[u, phantom, "\cup"] \arrow[r, phantom, "\subseteq"] & L_0 = K(c_0,\dots,c_{n-1}) \arrow[u, dash] \end{tikzcd}$$

Note φ is 1-1 because $\mathrm{tr.deg}_K\, K[\text{roots of } f(X)]$ is n. Thus $L = K(V)$

<u>Claim:</u> $\mathrm{Gal}(L/L_0) = GL_{\mathbb{F}_q}(E) =: G$. <u>Proof:</u> For the G-action on $W = E^*$ we have $G \xrightarrow{\sim} GL_{\mathbb{F}_q}(W)$ isomorphism. The G-action on L fixes K and also $c_0,\dots,c_{n-1}$ (since they are symmetric fns in the elts of W). Thus $G \subseteq \mathrm{Gal}(L/L_0)$.
Conversely any $\sigma \in \mathrm{Gal}(L|L_0)$ is L_0-linear, so $\mathbb{F}_q$-linear and permutes the roots of $f(X)$, and so acts an elt of $GL_{\mathbb{F}_q}(E)$ on W, and is determined by its action on W.
The claim is proved.

By the standard procedure for determining invariant rings, it now follows that $K[V]^G = K[c_0,\dots,c_{n-1}]$. Indeed (a) because of $f(X)$, $K[V]$ is integral over $K[c_0,\dots,c_{n-1}]$; (b) By (a) $K[c_0,\dots,c_{n-1}]$ is a polynomial ring and so normal; (c) $K(c_0,\dots,c_{n-1})$ is the fixed field of G for its action on L. QED

Explicitly writing the Dickson invariants (for $GL_n(\mathbb{F}_q)$)

Recall that the Dickson invariants are c_j, $j = 0, 1, \dots, n-1$, and

$$f(X) = X^{q^n} - c_{n-1} X^{q^{n-1}} + c_{n-2} X^{q^{n-2}} \pm \dots + (-1)^i c_{n-i} X^{q^{n-i}} \pm \dots + (-1)^n c_0 X^{q^0}$$

$$= \prod_{w \in W} (X - w).$$

To denote dependence on n, let's write $c_{n,j}$ instead of c_j.

Recall that W is the space of all linear forms on E, where $GL_n(\mathbb{F}_q) = GL_{\mathbb{F}_q}(E)$.

To understand the relation between $c_{n,j}$ and $c_{m,j}$ for $m \le n$ we restrict ~~to~~ — so to speak — the polynomial $f(X)$ to an m-dim. subspace E' of E. We see that

$$f_n(X)\big|_{E'} = f_m(X)^{q^{n-m}}$$

Equating ~~two~~ the $X^{q^{n-i}}$ terms: $(-1)^i c_{n,n-i} X^{q^{n-i}} = \left((-1)^i c_{m,m-i} X^{q^{m-i}}\right)^{q^{n-m}}$

$\therefore$ So $c_{n,n-i}\big|_{E'} = c_{m,m-i}^{q^{n-m}}$ for ~~[illegible]~~ $1 \le i \le m$

We are now ready to deduce an explicit expression for $c_j = c_{n,j}$

$$\boxed{c_{n,j} \underset{\text{upto sign}}{=} \sum_{\substack{\text{sum over all codim } j \\ \text{subspaces of } E \\ (E')}} \prod_{\substack{w \in E^* \\ w|_{E'} \neq 0}} w}$$

Proof: Both sides are hom. of degree $q^n - q^j$. The RHS is invariant, so is a multiple of $c_{n,j}$ (Tutorial 5.1). To compute this coeff restrict $c_{n,j}$ ~~both sides~~ to E' (where E' is some subspace of codim j). By ~~$c_{n,j}$~~ what has been said above $c_{n,j}\big|_{E'} = c_{n-j,0}^{q^j}$

The right side is also $c_{n-j,0}^{q^j}$ ~~since~~ (upto the sign $(-1)^{n-j}$). So the coefficient must be 1. QED