THE HASSE–DAVENPORT RELATION

1. Environment: Field, Traces, Norms

Let p be prime and let our ground field be

$$F_o = \mathbb{F}_p.$$

Let $q = p^r$ for some $r \geq 1$, and let the smaller of our two main fields be

$$F = \mathbb{F}_q.$$

The map

$$\sigma_p : F \longrightarrow F, \quad \sigma_p(t) = t^p$$

is an automorphism of F, and the group of automorphisms of F is the cyclic group of order r generated by σ_p,

$$\mathrm{Aut}(F) = \langle \sigma_p \rangle = \{1, \sigma_p, \sigma_p^2, \cdots, \sigma_p^{r-1}\}.$$

All such automorphisms fix F_o pointwise, and conversely any element of F that is fixed by the automorphisms lies in F_o. It suffices to check whether an element of F is fixed by the generator σ_p.

The **trace** function from F to F_o symmetrizes each element additively by summing it and all of its automorphisim-conjugates,

$$\mathrm{tr}_{F/F_o} : F \longrightarrow F_o, \quad \mathrm{tr}_{F/F_o}(t) = \sum_{\sigma \in \mathrm{Aut}(F)} \sigma(t).$$

Note that indeed $\mathrm{tr}(t)$ lies in F_o because it is fixed by automorphisms. The trace is an additive homomorphism, i.e.,

$$\mathrm{tr}_{F/F_o}(t + t') = \mathrm{tr}_{F/F_o}(t) + \mathrm{tr}_{F/F_o}(t'), \quad t, t' \in F.$$

Similarly, the **norm** function from F to F_o symmetrizes each element multiplicatively,

$$N_{F/F_o} : F \longrightarrow F_o, \quad N_{F/F_o}(t) = \prod_{\sigma \in \mathrm{Aut}(F)} \sigma(t).$$

The norm is a multiplicative homomorphism,

$$N_{F/F_o}(tt') = N_{F/F_o}(t) N_{F/F_o}(t'), \quad t, t' \in F^\times.$$

Fix some $s \geq 1$ and let the larger of our two main fields be

$$K = \mathbb{F}_{q^s}.$$

Note that K contains F as a subfield.

Since also $K = \mathbb{F}_{p^{rs}}$, the previous discussion of trace and norm applies verbatim with rs in place of r to give

$$\mathrm{tr}_{K/F_o} : K \longrightarrow F_o, \quad \mathrm{tr}_{K/F_o}(t) = \sum_{\sigma \in \mathrm{Aut}(K)} \sigma(t)$$

and

$$N_{K/F_o} : K \longrightarrow F_o, \quad N_{K/F_o}(t) = \prod_{\sigma \in \mathrm{Aut}(K)} \sigma(t).$$

But also, we now have a **relative** trace and norm. The map

$$\sigma_q : K \longrightarrow K, \quad \sigma_q(t) = t^q$$

is an automorphism of K that fixes F, and the group of such automorphisms of F is the cyclic group of order s generated by σ_q,

$$\mathrm{Aut}_F(K) = \langle \sigma_q \rangle = \{1, \sigma_q, \sigma_q^2, \cdots, \sigma_q^{s-1}\}.$$

All such automorphisms fix F pointwise and any element of K that is fixed by the automorphisms lies in F, and it suffices to check whether an element of K is fixed by σ_q.

The relative trace function from K to F is

$$\mathrm{tr}_{K/F} : K \longrightarrow F, \quad \mathrm{tr}_{K/F}(t) = \sum_{\sigma \in \mathrm{Aut}_F(K)} \sigma(t),$$

and the relative norm function from K to F is

$$N_{K/F} : K \longrightarrow F, \quad N_{K/F}(t) = \prod_{\sigma \in \mathrm{Aut}_F(K)} \sigma(t).$$

The relative trace is again additive and the relative norm is again multiplicative, and the traces and norms compose as nicely as they possibly could,

$$\mathrm{tr}_{K/F_o} = \mathrm{tr}_{F/F_o} \circ \mathrm{tr}_{K/F} \qquad \text{and} \qquad N_{K/F_o} = N_{F/F_o} \circ N_{K/F}.$$

2. Additive Characters, Multiplicative Characters, Gauss Sums

Recall that $F_o = \mathbb{F}_p$. Let $\zeta_p = e^{2\pi i/p} \in \mathbb{C}$. An additive character of F_o is

$$\psi_o : F_o \longrightarrow \mathbb{C}^\times, \quad \psi_o(t) = \zeta_p^t.$$

The corresponding additive character of F is

$$\psi_F : F \longrightarrow \mathbb{C}^\times, \quad \psi_F = \psi_o \circ \mathrm{tr}_{F/F_o},$$

and the corresponding additive character of K is

$$\psi_K : K \longrightarrow \mathbb{C}^\times, \quad \psi_K = \psi_F \circ \mathrm{tr}_{K/F},$$

Given also a nontrivial multiplicative character of F,

$$\chi_F : F^\times \longrightarrow \mathbb{C}^\times,$$

the corresponding multiplicative character of K is

$$\chi_K : K^\times \longrightarrow \mathbb{C}^\times, \quad \chi_K = \chi_F \circ N_{K/F}.$$

Definition 2.1. *The* **Gauss sum** *of χ_F is*

$$\tau(\chi_F) = \sum_{t \in F} \chi_F(t)\psi_F(t),$$

and the Gauss sum of χ_K is

$$\tau(\chi_K) = \sum_{t \in K} \chi_K(t)\psi_K(t).$$

Here we are tacitly defining $\chi(0) = 0$. Alternatively, we could sum over $t \in F^\times$ for the first Gauss sum and similarly for the second.

3. Gauss Sum Terms and Minimal Polynomials

Let t be a nonzero element of K. Let H be the subgroup of $\mathrm{Aut}_F(K)$ that fixes t. Then H takes the form

$$H = \langle \sigma_q^d \rangle \quad \text{for some } d \mid s.$$

Thus t has d distinct conjugates in K, including itself. Denote these conjugates t_1 through t_d where $t_1 = t$. Then

$$\mathrm{tr}_{K/F}(t) = (s/d)(t_1 + \cdots + t_d) \quad \text{and} \quad N_{K/F}(t) = (t_1 \cdots t_d)^{s/d}.$$

Also, consider the polynomial

$$f(X) = \prod_{i=1}^{d}(X - t_i) = X^d - (t_1 + \cdots + t_d)X^{n-1} + \cdots + (-1)^d(t_1 \cdots t_d).$$

Certainly $f(t) = 0$ since $t = t_1$. Also, because any automorphism σ of K over F permutes the conjugates of t, the product form of $f(X)$ shows that it is invariant when its coefficients are passed through any such σ. Thus the coefficients of f lie in the smaller field F. In fact $f(X)$ is the smallest monic polynomial in $F[X]$ satisfied by t, making it irreducible. The polynomial $f(X)$ is the **minimal polynomial** of t over F.

Rewrite the minimal polynomial of t as

$$f(X) = X^d - c_1X^{d-1} + \cdots + (-1)^d c_d$$

Then $(s/d)c_1 = \mathrm{tr}_{K/F}(t)$ and $c_n^{s/d} = N_{K/F}(t)$, and so

$$\begin{aligned}(\psi_F(c_1)\chi_F(c_d))^{s/d} &= \psi_F((s/d)c_1)\chi_F(c_d)^{s/d} \\ &= \psi_F(\mathrm{tr}_{K/F}(t))\chi_F(N_{K/F}(t)) \\ &= \psi_K(t)\chi_K(t),\end{aligned}$$

giving a term of the Gauss sum $\tau(\chi_K)$. And furthermore, since t and its conjugates all have the same trace and norm and hence all have the same ψ_K- and χ_K-values,

$$d(\psi_F(c_1)\chi_F(c_d))^{s/d} = \sum_{i=1}^{d} \psi_K(t_i)\chi_K(t_i).$$

Let $\mathcal{MI}$ denote the set of monic irreducible polynomials in $F[X]$. Each $t \in K$ satisfies some $f \in \mathcal{MI}$ with $\deg(f) \mid s$, and conversely each such $f \in \mathcal{MI}$ divides $X^{q^s} - X$ so that its roots lie in $K = \mathrm{spl}_F(X^{q^s} - X)$. If $f \in \mathcal{MI}$ is specified, let $d = \deg(f)$ and let c_1 and c_d be the coefficients of f as displayed in the previous paragraph. Then the previous display and the reasoning of this paragraph combine to give the following formula.

Proposition 3.1. *The Gauss sum for χ_K where $K = \mathbb{F}_{q^s}$ is*

$$\tau(\chi_K) = \sum_{\substack{f \in \mathcal{MI} \\ d \mid s}} d(\psi_F(c_1)\chi_F(c_d))^{s/d}.$$

4. An Euler Factorization for Polynomials

The calculations of the previous section suggest a general definition.

Definition 4.1. *Let $\mathcal{M}$ denote the set of monic polynomials in $F[X]$, not necessarily irreducible. Define a function*

$$\lambda : \mathcal{M} \longrightarrow \mathbb{C}^\times$$

as follows: For any $f(X) = X^d - c_1X^{d-1} + \cdots + (-1)^d c_d \in \mathcal{M}$,

$$\lambda(f) = \psi_F(c_1)\chi_F(c_d).$$

Note that in particular, $\lambda(1) = \psi_F(0)\chi_F(1) = 1$.

A little algebra shows that λ is multiplicative,

$$\lambda(fg) = \lambda(f)\lambda(g) \quad \text{for all monic } f, g \in \mathcal{M}.$$

That is, λ gathers the additive character ψ_F and the multiplicative character χ_F into a single multiplicative character on the monoid $\mathcal{M}$. (A monoid is like a group but without inverses.)

Proposition 4.2. *The following Euler factorization identity holds for any multplicative function $\lambda : \mathcal{M} \longrightarrow \mathbb{C}^\times$,*

$$\sum_{f\in\mathcal{M}} \lambda(f)T^{\deg f} = \prod_{f\in\mathcal{MI}} (1 - \lambda(f)T^{\deg f})^{-1}.$$

Furthermore, for the particular λ of the previous definition, the left side of the previous display simplifies to

$$\sum_{f\in\mathcal{M}} \lambda(f)T^{\deg f} = 1 + \tau(\chi_F)T.$$

Proof. The fact that every monic polynomial factors uniquely into monic irreducibles gives the crucial third equality (in which the symbol f changes its meaning from a general monic irreducible polynomial on the left side of the equality to a general monic polynomial on the right side) in the calculation

$$\begin{aligned}
\prod_{f\in\mathcal{MI}} (1 - \lambda(f)T^{\deg f})^{-1} &= \prod_{f\in\mathcal{MI}} \sum_{n\geq 0} (\lambda(f))^n T^{n\deg f} \\
&= \prod_{f\in\mathcal{MI}} \sum_{n\geq 0} \lambda(f^n)T^{\deg(f^n)} \\
&= \sum_{f\in\mathcal{M}} \lambda(f)T^{\deg f}.
\end{aligned}$$

This gives the Euler factorization. For the second part, we have

$$\sum_{f\in\mathcal{M}} \lambda(f)T^{\deg f} = \sum_{n\geq 0} \sum_{\substack{f\in\mathcal{M}\\ d=n}} \lambda(f)T^{\deg f}.$$

For $n = 0$ the inner sum is 1. For $n = 1$, the monic irreducible polynomials are $f(X) = X - t$ for all $t \in F$, with $c_1 = c_d = t$, and so the inner sum is

$$\sum_{\substack{f\in\mathcal{M}\\ d=1}} \lambda(f)T = \sum_{t\in F} \lambda(X - t)T = \sum_{t\in F} \psi_F(t)\chi_F(t)T = \tau(\chi_F)T.$$

For $n \geq 2$, note that for each choice of c_1 and c_n in F there are q^{n-2} monic polynomials with those coefficients. Thus

$$\sum_{\substack{f \in \mathcal{M} \\ d=n}} \lambda(f)T = q^{n-2} \sum_{c_1, c_n \in F} \psi_F(c_1)\chi_F(c_n) = q^{n-2} \sum_{c_1 \in F} \psi_F(c_1) \sum_{c_n \in F} \chi_F(c_n).$$

But both character sums are zero (for the second sum it is relevant that χ_F is nontrivial), and so the entire expression vanishes. □

5. The Hasse–Davenport Relation

Theorem 5.1 (Hasse–Davenport Relation). *The relation between the Gauss sums $\tau(\chi_K)$ and $\tau(\chi_F)$ is*

$$-\tau(\chi_K) = (-\tau(\chi_F))^s.$$

Proof. From the previous proposition we have the relation

$$1 + \tau(\chi_F)T = \prod_{f \in \mathcal{MI}} (1 - \lambda(f)T^{\deg(f)})^{-1}.$$

Take logarithmic derivatives and multiply by T,

$$\frac{\tau(\chi_F)T}{1 + \tau(\chi_F)T} = \sum_{f \in \mathcal{MI}} \frac{\deg(f)\lambda(f)T^{\deg(f)}}{(1 - \lambda(f)T^{\deg(f)})},$$

and then expand the geometric series,

$$\sum_{n \geq 1} (-1)^{n-1} \tau(\chi_F)^n T^n = \sum_{f \in \mathcal{MI}} \sum_{d \geq 1} \deg(f)\lambda(f)^d T^{d \deg(f)}.$$

Equate the coefficients of T^s,

$$-(-\tau(\chi_F)^s) = \sum_{\substack{f \in \mathcal{MI} \\ d|s}} d\lambda(f)^{s/d}.$$

The right side is $\tau(\chi_K)$ by Proposition 3.1, so the proof is complete. □