Title

D. Zack Garza

Contents

1 | Lecture 13

Recall that we previously looked at the regular function fields: we took a function field in one variable and considered the class of function fields for which we could take any extension of the constant field that we wanted. As long as the ground field is perfect, being regular is equivalent to the constant subfield being k itself. However, we haven't done anything with them yet!

If you take an algebraic closure of the finite ground field $\mathbb{F}_q$, there is a unique subextension of degree r for every r, so we call that $\mathbb{F}_q^r$. The extension $\mathbb{F}_q^r/\mathbb{F}_q$ is cyclic galois, with a geometric Frobenius $x \to x^q$. Note that $\mathbb{F}_q^r$ is the fixed field of F^r, the rth power of the Frobenius map. We set $K_r \coloneqq K\mathbb{F}_q^r$, which is a regular function field over $\mathbb{F}_q^r$. Note that we could view this as a function field just over $\mathbb{F}_q$, but it would not be regular. Then K_r/K is a degree r arithmetic extension of function fields.

Question: What happens to places when making this scalar extension? I.e., how to places in K decompose in K_r?

Remark 1.0.1 : This is related to an Algebraic Number Theory I problem: for $v \in \Sigma(K_{/\mathbb{F}_q})$ above an affine Dedekind domain R such that $v \in \Sigma(K/R)$, let S be the integral closure of K in K_r. Then we want to factor $p_v S$?

Not quite sure.

Lemma 1.1 ***(Key lemma about how places split.).***
Suppose $d \coloneqq \deg(v)$. Then K_r/K is galois, so we have $efg = r$. In fact, $c = 1$, so $f = \dfrac{r}{\gcd(d,r)}$ and $g = \gcd(d,r)$ and each place $w \in \Sigma(K_r/\mathbb{F}_q^r)$ has degree $\dfrac{d}{\gcd(d,r)}$.

Remark 1.0.2 : We have the following cases:

- The extension is *inert* iff $\gcd(d,r) = 1$,
- The extension *splits completely* iff $r \mid d$,
- All w dividing v have degree 1 iff $d \mid r$.

The last thing we proved was that the degree zero divisor class group is finite when we're over a finite ground field. Why is this true? Whenever there is a divisor of degree n, then the set of degree n divisors is a coset of the degree zero divisors, all of which have the same cardinality. We proved finiteness using the Riemann-Roch theorem, using the fact that the set of *effective* degree n divisors is finite for all n.

The next main topic will be the zeta function, which keeps track of three equivalent packets of

information: A_n, the number of effective divisors of degree n, the number of places of degree d (since an effective divisor is a linear combination of these), and N_r the number of degree 1 points in the degree r extension, i.e. the number of $\mathbb{F}_q^r$ rational points.

Lemma 1.2 ***(?).***
Suppose $C \in \mathrm{Cl}(K)$, then

- The number of effective divisors $D \in [C]$ is given by

$$\frac{q^{\ell(C)}-1}{q-1},$$

  where $\ell(C)$ is the dimension of the linear system associated to the divisor class C, and this is the dimension of a projective space over $\mathbb{F}_q$.

- For all $n > 2g-2$ with $\delta \mid n$, we have

$$A_n = h\left(\frac{q^{n+1-g}-1}{q-1}\right).$$

Proof (?).
Proof of (a): The set of effective divisors linearly equivalent to D is naturally viewed as the projectivization $\mathbb{P}\mathcal{L}(D)$ of the one-dimensional subspaces of the linear system of that divisor class. It is then a fact that the number of elements in a d-dimensional vector space over $\mathbb{F}_q$ has dimension precisely $\frac{q^d-1}{q-1}$ elements.
The projectivization comes in because two different functions have the same divisor if one of them is a constant multiple of the other. Note that the number of elements is computed as the number of nonzero elements divided by the number of nonzero scalars.
Proof of (b): This will come out of the Riemann-Roch theorem. In order to compute the number of divisors in a divisor class, you need to know the dimension of the linear system, which is not easy in general. However, if the divisor class has sufficiently large degree, the Riemann-Roch theorem tells you exactly what it is. As long as $n > 2g-2$, there is no correction term, and we

■