Algebraic-Geometric Codes **Fall 2024/5**

Recitation 6: Extension of Places, Divisors, Trace and Norm

Scribe: Tomer Manket

1 Extension of Places

Theorem 1. *Let $F_0 \subseteq F$ be fields and let L be an algebraically closed field. Then every place $\varphi_0\colon F_0 \to L \cup \{\infty\}$ can be extended to a place $\varphi\colon F \to L \cup \{\infty\}$.*

Corollary 2. *Let F/K be field extension. Let $x \in F$ be transcendental over K. Then there exist valuations ν, ν' on F which trivial on K such that $\nu(x) > 0$ and $\nu'(x) < 0$.*

Proof. Let L be an algebraic closure of K and consider the place $\varphi_0\colon K(x) \to L \cup \{\infty\}$ given by

$$\varphi_0\left(\frac{f(x)}{g(x)}\right) = \begin{cases} \frac{f(0)}{g(0)} & x \nmid g(x) \text{ in } K[x] \\ \infty & \text{otherwise} \end{cases}$$

(where $f, g \in K[x]$ are coprime and $g \neq 0$). Then φ_0 is the identity on K and $\varphi_0(x) = 0$. Applying Theorem 1 to φ_0 (with $F_0 = K(x) \subseteq F$), we can extend it to a place $\varphi\colon F \to L \cup \{\infty\}$ of F. Its corresponding valuation ν is a valuation on F which trivial on K and satisfies $\nu(x) > 0$. As $x^{-1} \in F$ is also transcendental over K, we can similarly find a valuation ν' with $\nu'(x^{-1}) > 0$, i.e. $\nu'(x) < 0$. □

2 Divisors

Let F/K be a function field.

Definition 3. A divisor of F/K is a formal sum $\sum_{\mathfrak{p} \in \mathbb{P}_F} n_\mathfrak{p} \mathfrak{p}$, where each $n_\mathfrak{p} \in \mathbb{Z}$ and $n_\mathfrak{p} = 0$ for almost all $\mathfrak{p} \in \mathbb{P}_F$. The set $\mathcal{D}$ of all divisors is a group (with pointwise-addition).

Theorem 4. *For each $x \in F^\times$ we define $(x) := \sum_{\mathfrak{p} \in \mathbb{P}_F} \nu_\mathfrak{p}(x)\mathfrak{p}$. Then $(x) \in \mathcal{D}$ and is called a* principal divisor*. The set of principal divisors $\mathcal{P} = \{(x) \mid x \in F^\times\}$ is a subgroup of $\mathcal{D}$.*

Definition 5. The quotient group $\mathcal{C} = \mathcal{D}/\mathcal{P}$ is called the *divisor class group* of F/K.

Exercise. Show that every divisor of degree zero of the rational function field $K(x)/K$ is principal. Conclude that the divisor class group of $K(x)/K$ is $\mathcal{C} \cong \mathbb{Z}$.

Proof. Let $\mathfrak{a} \in \mathcal{D}$ be a divisor of $K(x)/K$ with $\deg \mathfrak{a} = 0$ and let $S = \mathrm{supp}(\mathfrak{a}) \backslash \{\mathfrak{p}_\infty\}$. Then $\mathfrak{a} = \sum_{\mathfrak{p} \in S} n_\mathfrak{p} \mathfrak{p} + m\mathfrak{p}_\infty$. Since $\deg \mathfrak{a} = 0$ we have

$$\sum_{\mathfrak{p} \in S} n_\mathfrak{p} \deg \mathfrak{p} + m = 0 \implies m = -\sum_{\mathfrak{p} \in S} n_\mathfrak{p} \deg \mathfrak{p}.$$

Let $f = \prod_{\mathfrak{p} \in S} \mathfrak{p}^{n_\mathfrak{p}} \in K(x)$. Then $\mathfrak{a} = (f)$:

Indeed, for $\mathfrak{p} \in S$ we have $\nu_\mathfrak{p}(\mathfrak{a}) = n_\mathfrak{p} = \nu_\mathfrak{p}(f)$. For $\mathfrak{p} \notin S \cup \{\mathfrak{p}_\infty\}$ we have $\nu_\mathfrak{p}(\mathfrak{a}) = 0 = \nu_\mathfrak{p}(f)$. Finally,

$$\nu_\infty(\mathfrak{a}) = m = -\sum_{\mathfrak{p} \in S} n_\mathfrak{p} \deg \mathfrak{p} = -\deg f = \nu_\infty(f).$$

Thus $\mathfrak{a}$ is principal. To conclude, consider the group homomorphism $\deg \colon \mathcal{D} \to \mathbb{Z}$. By the first part, its kernel is contained in $\mathcal{P}$. Since every principal divisor has degree 0, the kernel is exactly $\mathcal{P}$. Since there exists a prime divisor of degree 1 in $K(x)/K$ (for example, $\mathfrak{a} = \mathfrak{p}_x$) the image is $\mathbb{Z}$. Hence by the first isomorphism theorem, $C = \mathcal{D}/\mathcal{P} \cong \mathbb{Z}$. □

3 Trace and Norm

Let L/K be a field extension of degree $[L : K] = n < \infty$. Each element $\alpha \in L$ yields a K-linear map $\mu_\alpha \colon L \to L$ defined by $x \mapsto \alpha \cdot x$. Indeed, for every $x, y \in L$ and $c \in K$,

$$\mu_\alpha(x + y) = \alpha(x + y) = \alpha x + \alpha y = \mu_\alpha(x) + \mu_\alpha(y)$$

and

$$\mu_\alpha(cx) = \alpha \cdot (cx) = c \cdot (\alpha x) = c \cdot \mu_\alpha(x).$$

Let $M_\alpha \in K^{n \times n}$ be the matrix representing μ_α w.r.t some basis $\{v_1, \dots, v_n\}$ of L over K. That is, if $\mu_\alpha(v_i) = \alpha \cdot v_i = \sum_{j=1}^n a_{ij} v_j$ with $a_{ij} \in K$, then $M_\alpha = (a_{ij})$.

Definition 6. The *trace* $\mathrm{Tr}_{L/K} \colon L \to K$ is the map given by

$$\mathrm{Tr}_{L/K}(\alpha) := \mathrm{Trace}(M_\alpha).$$

Definition 7. The *norm* $\mathrm{N}_{L/K} \colon L \to K$ is the map given by

$$\mathrm{N}_{L/K}(\alpha) := \det(M_\alpha).$$

Remark 1. Since conjugate matrices have the same trace and determinant, these definitions are independent of the choice of the basis of L/K.

Let $\alpha \in L$. Then $K \subseteq K(\alpha) \subseteq L$. Let $s := [L : K(\alpha)]$ and $r = [K(\alpha) : K]$ so that $n = [L : K] = rs$. The minimal polynomial of α over K then takes the form

$$p_\alpha(X) = X^r + a_{r-1} X^{r-1} + \ldots + a_1 X + a_0 \in K[X].$$

Theorem 8. *In the setting above,*

$$\mathrm{Tr}_{L/K}(\alpha) = -sa_{r-1} \quad \textit{and} \quad \mathrm{N}_{L/K}(\alpha) = (-1)^n a_0^s.$$

Moreover, if L/K is Galois with $G = \mathrm{Gal}(L/K)$, then

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha) \quad \textit{and} \quad \mathrm{N}_{L/K}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha). \tag{1}$$

Proof. We only prove in case $[K(\alpha) : K] = n$, i.e. $L = K(\alpha)$, $r = n$ and $s = 1$ (for the full proof, see Section 5 in [1]). In this case, we can take the basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ of L over K. Since $\mu_\alpha(\alpha^i) = \alpha^{i+1}$ for $0 \leq i < n-1$ and

$$\mu_\alpha(\alpha^{n-1}) = \alpha^n = -a_0 - a_1\alpha - \ldots - a_{n-1}\alpha^{n-1},$$

we obtain

$$M_\alpha = \begin{pmatrix} 0 & \ldots & 0 & -a_0 \\ 1 & \ldots & 0 & -a_1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \ldots & 1 & -a_{n-1} \end{pmatrix}.$$

Thus,

$$\mathrm{Tr}_{L/K}(\alpha) = \mathrm{trace}(M_\alpha) = -a_{n-1} \quad \textit{and} \quad \mathrm{N}_{L/K}(\alpha) = \det(M_\alpha) = (-1)^n a_0.$$

Moreover, if L/K is Galois, then

$$p_\alpha(X) = \prod_{\sigma \in G} (X - \sigma(\alpha))$$

so that $-a_{n-1} = \sum_{\sigma \in G} \sigma(\alpha)$ and $a_0 = (-1)^n \prod_{\sigma \in G} \sigma(\alpha)$, from which (1) follows. □

References

[1] Keith Conrad. TRACE AND NORM. URL: https://kconrad.math.uconn.edu/blurbs/galoistheory/tracenorm.pdf.