Algebraic Number Theory, L2

Hypersurface S in the projective space $\mathbb{P}_n$

– makes sense for a homogeneous polynomial $P \in F[x_0, x_1, \dots, x_n]$, i.e. $P(x_0, x_1, \dots, x_n) = \sum_{\substack{\bar{a} \in \mathbb{N}_0^{n+1} \\ \|\bar{a}\| = d}} c_{\bar{a}} x^{\bar{a}}$ where $\bar{a} = (a_0, a_1, \dots, a_n) \in \mathbb{N}_0^{n+1}$ ($\mathbb{N}_0 = \{0, 1, 2, \dots\}$), $\|\bar{a}\| = a_0 + a_1 + \dots + a_n$, $c_{\bar{a}} \in F$ are the coefficients of P, and $x^{\bar{a}} = x_0^{a_0} x_1^{a_1} \dots x_n^{a_n}$.

Then the definition $S = \{\bar{\alpha} = [\alpha_0 : \alpha_1 : \dots : \alpha_n] \in \mathbb{P}_n \mid P(\bar{\alpha}) = 0_F\}$ is a correct one because for any $\alpha_i \in F$ and $\lambda \in F^\times$, $P(\lambda\alpha_0, \lambda\alpha_1, \dots, \lambda\alpha_n) = \lambda^d P(\alpha_0, \alpha_1, \dots, \alpha_n)$ – P either vanishes on every representative of the projective point, or is $\neq 0_F$ on all of them.

Every polynomial $P \in F[x_1, \dots, x_n]$ can be homogenized to yield the polynomial

$\overline{P}(x_0, x_1, \dots, x_n) := x_0^d P(x_1/x_0, x_2/x_0, \dots, x_n/x_0)$ where $d = \deg P$. From $\overline{P}$ we get P back by the formula $P(x_1, \dots, x_n) := \overline{P}(1_F, x_1, \dots, x_n)$. $\overline{P}$ is, of course, homogeneous with degree $d = \deg P$. What is the difference ~~of~~ between the <u>affine hypersurface</u> S defined by P and the <u>projective hypersurface</u> $\overline{S}$ defined by $\overline{P}$?

$$S = \{(\alpha_1, \dots, \alpha_n) \in \overset{F^n}{\overset{\|}{A_n}} \mid P(\alpha_1, \dots, \alpha_n) = 0_F\},$$

$$\overline{S} = \{(\alpha_0 : \dots : \alpha_n) \in \mathbb{P}_n \mid \overline{P}(\alpha_0, \alpha_1, \dots, \alpha_n) = 0_F\}.$$

$S \hookrightarrow \overline{S}$ by the inclusion map

$S \underset{\text{''}}{\subset}\text{''} \overline{S} \qquad (\alpha_1, \alpha_2, \dots, \alpha_n) \mapsto (1_F : \alpha_1, \alpha_2, \dots, \alpha_n)$.

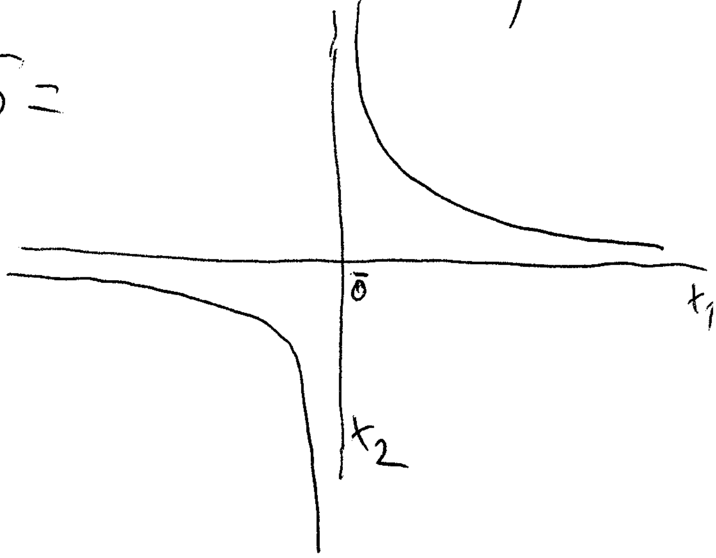
In addition to S, the h. $\overline{S}$ contains the "points of S in infinity", i.e. $\overline{S} \setminus S =$

$$= \{(0_F : \alpha_1 : \dots : \alpha_n) \in \mathbb{P}_n \mid \overline{P}(0_F, \alpha_1, \dots, \alpha_n) = 0_F\}.$$

$\boxed{\text{Example}}$ $F = \mathbb{R}$ (the real numbers), $n = 2$,

$P(x_1, x_2) = x_1 x_2 - 1 \rightsquigarrow S =$

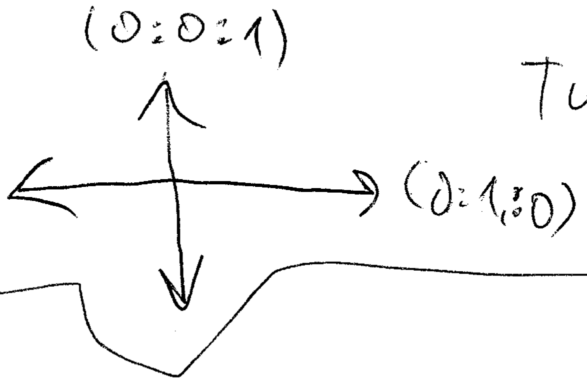
$= \left\{ \left(x_1, \frac{1}{x_1} \right) \mid x_1 \in \mathbb{R}^\times \right\}.$



$\bar{P}(x_0, x_1, x_2) = x_1 x_2 - x_0^2$

$$\rightsquigarrow \bar{S} = \underbrace{\left\{ \left(1 : x_1 : \tfrac{1}{x_1} \right) \mid x_1 \in \mathbb{R}^\times \right\}}_{\text{"="} S} \cup \underbrace{\left\{ (0:1:0), (0:0:1) \right\}}$$

Two points of S in infinity.



the zeta function of any affine (or projective) hypersurface... We denote the aff. and proj. hypersurfaces defined by the polynomial $P \in F[x_1, \dots, x_n]$ by $S_P(F)$ and $\bar{S}_P(F)$, respectively.

Let $F=\mathbb{F}_q$, q is a prime power $q=p^r$, be a finite field ~~with q elements~~ and $K=\mathbb{F}_{q^{\hat{s}}}$, $\hat{s}\in\mathbb{N}$, be its extension with degree $\hat{s}=[K:F]$.

Let $P\in F[x_1,\dots,x_n]$ and for $s\in\mathbb{N}$,

$$N_s := \# S_p(K)$$

$$= \#\{(x_1,\dots,x_n)\in K^n \mid P(x_1,\dots,x_n)=0_K\}.$$

<u>the zeta function of the hypersurface defined by P</u> is

$$Z(S_P/\mathbb{F}_q;X) := \exp\left(\sum_{s=1}^{\infty}\frac{N_s X^s}{s}\right)\in\mathbb{Q}[[X]]$$

$\boxed{\text{Proposition 2}}$ $Z(S_{P(\bar{X})}/\mathbb{F}_q;X)\in\mathbb{Z}[[X]]$, in fact $\in\mathbb{N}_0[[X]]$

<u>Proof.</u> Next time.

$\boxed{\text{Proposition 3}}$ $\underbrace{[X^j]\,Z(S_{P(\bar{X})}/\mathbb{F}_q;X)}_{\text{the coefficient of } X^j \text{ in } \dots,\ j\in\mathbb{N}_0}\leq q^{nj}$.

Proof. $\Longrightarrow \exp\left(\sum_{s=1}^{\infty} \frac{N_s x^s}{s}\right) \preceq \exp\left(\sum_{s=1}^{\infty} \frac{q^{ns} x^s}{s}\right) =$

$$= \exp\left(\log \frac{1}{1-\cancel{x}\, q^n \cancel{x}}\right) = \frac{1}{1-q^n x} = \sum_{s=1}^{\infty} q^{ns} x^s$$

where $\preceq$ means coefficient-wise majorization of formal power series ($N_s \leq \# A_n(\mathbb{F}_{q^s}) = (q^s)^n = q^{ns}$). $\boxtimes$