

LEMMA 8.1. *Let p be an odd prime. Let ζ be a primitive 8-th root of unity in $\overline{\mathbb{F}_p}$. That means, ζ is a root of $X^4 + 1 \in \mathbb{F}_p[X]$. Let us put $x = \zeta + \zeta^{-1}$. Then:*

- (1) $x^2 = 2$.
- (2) $x^p - x = 0$ if $p = \pm 1 \pmod{8}$.
- (3) $x^p + x = 0$ if $p = \pm 3 \pmod{8}$.
- (4) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

projective space and projective varieties.

DEFINITION 8.2. Let R be a ring. A polynomial $f(X_0, X_1, \dots, X_n) \in R[X_0, X_1, \dots, X_n]$ is said to be **homogeneous** of degree d if an equality

$$f(\lambda X_0, \lambda X_1, \dots, \lambda X_n) = \lambda^d f(X_0, X_1, \dots, X_n)$$

holds as a polynomial in $n + 2$ variables $X_0, X_1, X_2, \dots, X_n, \lambda$.

DEFINITION 8.3. Let k be a field.

- (1) We put

$$\mathbb{P}^n(k) = (k^{n+1} \setminus \{0\})/k^\times$$

and call it (the set of k -valued points of) the **projective space**.

The class of an element (x_0, x_1, \dots, x_n) in $\mathbb{P}^n(k)$ is denoted by $[x_0 : x_1 : \dots : x_n]$.

- (2) Let $f_1, f_2, \dots, f_l \in k[X_0, \dots, X_n]$ be homogenous polynomials. Then we set

$$V_h(f_1, \dots, f_l) = \{[x_0 : x_1 : x_2 : \dots : x_n]; f_j(x_0, x_1, x_2, \dots, x_n) = 0 \quad (j = 1, 2, 3, \dots, l)\}.$$

and call it (the set of k -valued point of) the **projective variety** defined by $\{f_1, f_2, \dots, f_l\}$.

(Note that the condition $f_j(x) = 0$ does not depend on the choice of the representative $x \in k^{n+1}$ of $[x] \in \mathbb{P}^n(k)$.)

THEOREM 8.4. *Let p be a prime, q be a power of p . Let $f(X_1, \dots, X_n) \in \mathbb{F}_q[X_1, \dots, X_n]$ be a polynomial of degree d . Let us put*

$$N = \#\{x = (x_1, x_2, \dots, x_n) \in \mathbb{F}_q^n; f(x) = 0\}.$$

Then we have

$$n > d \implies p|N.$$

For the proof we use the following lemma

LEMMA 8.5. *Let k be a positive integer. Then we have*

$$\sum_{c \in \mathbb{F}_q} c^k = \begin{cases} -1 & \text{if } (q-1)|k \\ 0 & \text{otherwise.} \end{cases}$$