

§51 Separable extensions

Problem : in positive characteristic ($\mathbb{Z}_p \subset F$ for some prime p) an irreducible polynomial $f(X) \in F[X]$ can have a root with multiplicity

Ex. $F = \mathbb{Z}_p(Y) = \left\{ \frac{f(Y)}{g(Y)} \mid f(Y), g(Y) \in \mathbb{Z}_p[Y] \right\}$

$$h(X) = X^p - Y \in F[X] \rightsquigarrow (X - Y^{1/p})^p = h(X)$$

(Fact : this does not happen for finite fields
Thms 51.13 and 14 and for characteristic 0 ($\mathbb{Q} \subset F$))

Lem. 51.11 $E \supset F$ finite extension

$$f(X) = a_0 + a_1 X + \dots + a_{n-1} X^{n-1} + X^n \in E[X]$$

(monic polynomial $\uparrow$)

Suppose $f(X)^m \in F[X]$ for some pos. int. m
such that $m \neq 0$ in F (any int for char. 0)

Then $f(X) \in F[X]$

Proof Step 1 $a_{n-1} \in F$

$$f(X)^m = (X^n + a_{n-1} X^{n-1} + \dots)^m$$

$$= X^{nm} + m a_{n-1} X^{nm-1} + \dots \in F[X]$$

$$m \neq 0 \rightsquigarrow a_{n-1} = \frac{1}{m} \cdot m a_{n-1} \text{ is also in } F$$

Step 2 $a_{n-2} \in F$

again expand $\underbrace{(X^n + a_{n-1} X^{n-1} + a_{n-2} X^{n-2} + \dots)}_{\text{in } F[X]}^m$

and look at the term of order $nm-2$

$$\rightsquigarrow \text{coeff. } m \cdot a_{n-2} + \underbrace{(\text{some polynomial of } a_{n-1})}_{\text{in } F}$$

$$\rightsquigarrow \text{use } \frac{1}{m} \text{ to get } a_{n-2} \in F$$

... continue with induction $\square$

Rem If $m = 0$ in F , above ex. $h(X) = X^p - Y$
would fail this lemma

Prop. (Cor 51.3) $f(X) \in F[X]$ irred. polynom.

$$\leadsto f(X) = c \prod_{i=1}^k (X - \alpha_i)^m$$

with $\begin{cases} \alpha_1, \dots, \alpha_k \text{ roots of } f(X) \text{ in } \bar{F} \\ c \in F \text{ (coeff. of highest order term)} \\ m: \text{ pos. integer} \end{cases}$

Proof idea take $\psi_{\alpha_i, \alpha_j}: F(\alpha_i) \rightarrow F(\alpha_j)$ and

extend it to an autom. $\tau: \bar{F} \rightarrow \bar{F}$ ($\tau(a) = a$ for $a \in F$)

If $(X - \alpha_i)^m$ divides $f(X)$ in $\bar{F}[X]$

$$\tau((X - \alpha_i)^m) = (X - \alpha_j)^m \text{ divides } \tau(f(X)) = f(X)$$

Cor. If $m \neq 0$ in F for the above m , ~~and $m \neq 1$~~

then $m = 1$.

$$\therefore g(X) = \prod_{i=1}^k (X - \alpha_i) \text{ satisfies } g(X)^m = \frac{f(X)}{c} \in F[X]$$

$\leadsto g(X) \in F[X] \leadsto$ by irreducibility $m = 1$

Def. $f(X) \in F[X]$ irred. polynom. is separable

if $f(X) = c \prod_{i=1}^k (X - \alpha_i)$ $\alpha_i \neq \alpha_j \in \bar{F}$

Def - Th'm (51.7, 51.10) $E \supset F$ finite extension

The following conditions are equivalent

- $E \supset F$ is separable : $[E:F] = \sum_{\dim_F E} \{ E:F \}$ num. of homs $E \xrightarrow{\sigma} \bar{F}$
- for each $\alpha \in E$, the min. polynom. $f(X) \in F[X]$ is separable

Proof idea Step 1 If $E = F(\alpha)$, then

$$\underbrace{[E:F]}_{\deg f = k \cdot m} = \underbrace{\{E:F\}}_k \cdot m \text{ if min. poly. } f(X) \text{ satisfies } f(X) = \prod_{i=1}^k (X - \alpha_i)^m$$

Step 2 In general $\{E:F\}$ divides $[E:F]$

$$\text{use } E \supset K \supset F \leadsto \{E:F\} = \{E:K\} \{K:F\} \quad (49.10)$$

§53 Galois theory

so far we have two kinds of extensions

- splitting extensions $E \supset F$

$\alpha \in E \leadsto$ min poly. $f(X) \in F[X]$ splits as

$$f(X) = \prod_{i=1}^k (X - \alpha_i)^{m_i} \quad \alpha_1, \dots, \alpha_k \in E$$

- separable extensions $E \supset F$

$\alpha \in E \leadsto$ min poly. $f(X) \in F[X]$ splits as

$$f(X) = \prod_{i=1}^k (X - \alpha_i) \quad \alpha_1, \dots, \alpha_k \in \bar{F}$$

What happens if we combine both?

Def. (cf. 53.1) $E \supset F$ is a Galois extension if it is both splitting and separable

(Rem. Fraleigh calls this normal but usually normal $\equiv$ splitting)

Overview of the Galois theory: if $E \supset F$ is a Galois extension, then

1. F agrees with $\{ \alpha \in E \mid \sigma(\alpha) = \alpha \text{ for } \sigma \in E_{G(E/F)} \}$

(in general we only have $F \subset E_{G(E/F)}$)

2. for any subextension $F \subset K \subset E$

$$H = \{ \sigma \in G(E/F) \mid \sigma(b) = b \text{ for } b \in K \}$$

satisfies $K = E_H$, ~~$G(K/F)$~~

this gives bijective corresp.

$$\{ \text{subextensions } F \subset K \subset E \} \leftrightarrow \{ \text{subgroups } H \subset G(E/F) \}$$

3. if $F \subset K$ is also Galois, then H is normal,
 $G(K/F) \cong G(E/F)/H$

(

The first part of the problem is to find the area of the rectangle.

Let the length of the rectangle be l and the width be w .

Then the area of the rectangle is given by the formula:

$$A = l \times w$$

where A is the area, l is the length, and w is the width.

Now, we are given that the length is 10 units and the width is 5 units.

$$l = 10, w = 5$$

Substituting these values into the area formula, we get:

$$A = 10 \times 5 = 50$$

Therefore, the area of the rectangle is 50 square units.

Next, we need to find the perimeter of the rectangle.

$$P = 2l + 2w$$

where P is the perimeter, l is the length, and w is the width.

Substituting the given values, we have:

$$P = 2(10) + 2(5) = 20 + 10 = 30$$

Thus, the perimeter of the rectangle is 30 units.

(

Finally, we need to find the diagonal of the rectangle.

$$d = \sqrt{l^2 + w^2}$$

where d is the diagonal, l is the length, and w is the width.

$$d = \sqrt{10^2 + 5^2} = \sqrt{100 + 25} = \sqrt{125} = 5\sqrt{5}$$

Therefore, the length of the diagonal is $5\sqrt{5}$ units.

In conclusion, the area is 50 square units, the perimeter is 30 units, and the diagonal is $5\sqrt{5}$ units.

These calculations are based on the given dimensions of the rectangle.

(

$$A = 50, P = 30, d = 5\sqrt{5}$$

Q.E.D.