§2.2.7: Separable polynomials and perfect fields

Definition. For a field K, a polynomial $f(x) \in K[x]$ is said to be separable over K if it has no repeated roots in its splitting field over K.

Example. $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ is separable over $\mathbb{Q}$, but not when regarded as a polynomial over $\mathbb{F}_3$:

$$f(x) = (x-2)^3 \in \mathbb{F}_3[x].$$

Example. $K = \mathbb{F}_2(t)$ and $f(x) = x^2 - t \in K[x]$. The splitting field of $L = K(\sqrt{t})$ of f over K has degree 2 over K, but

$$f(x) = x^2 - t = (x - \sqrt{t})^2 \in L[x],$$

so f is not separable. over $K = \mathbb{F}_2(t)$.

Lemma. Let K be any field and let $f \in K[x]$ with positive degree. Then the following are equivalent:

Tutorial

1. f is separable over K;
2. f and f' are relatively prime as elements in $K[x]$;
3. f has no repeated roots in any field extension L of K.

Proof. Let $f = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, $p_i \in K[x]$ irreducible, pairwise non-associates. Let L_f be the splitting field of f over K.

- 1) $\Rightarrow$ 2): For each j, f and p_j share at least one root $a_j \in L_f$. Then $f'(a_j) \neq 0$ implies that $p_j \nmid f'$. Thus f and f' have no common irreducible factors in $K[x]$, i.e., they are relatively prime in $K[x]$.
- 2) $\Rightarrow$ 3): f and f' are relatively prime in $K[x]$ implies that they are relatively prime in $L[x]$ for any extension $K \subset L$, so f has no repeated root in any extension L of K.
- 3) $\Rightarrow$ 1): trivial.

Q.E.D.

Perfect fields:

Definition. A field K is said to be perfect if every irreducible polynomial in $K[x]$ is separable.

Example. $K = \mathbb{F}_2[t]$ is not perfect, as $p(x) = x^2 - t \in K[x]$ is irreducible but not separable.

Theorem: A field K is perfect if and only if either one of the following holds:

1. $\mathrm{char}(K) = 0$;
2. $\mathrm{char}(K) = p > 0$ but the Frobenious homomorphism $\sigma : K \to K, \sigma(a) = a^p$ is an isomorphism, or, equivalently, surjective.

Proof. See lecture notes.

Corollary. A field of characteristic 0 is perfect; A finite field is perfect.

§2.2.8: Separable extensions and the Primitive Element Theroem

Definition. An algebraic extension $K \subset L$ is said to be separable if for every $a \in L$, the minimal polynomial of a over K is separable over K.

Lemma. Every finite extension of a perfect field is separable.

The Primitive Element Theroem. A finite separable extension $K \subset L$ is simple.

Proof: see lecture notes.

Corollary. If K is a perfect field, then very finite extension of K is simple.

Corollary. If K has characteristic 0 or is a fintie field, then very finite extension of K is simple.

We now turn to Chapter 3. Introduction to Galois Theory.

Today:

1. §3.2.1: Automorphism groups of field extensions and roots of polynomials

What we need from group theory in this chapter:

- Definition of groups an subgroups;
- For a set R, the group $R = \{1, 2, \cdots n\}$

$$\mathrm{Perm}(R) = \text{the set of all bijections from } R \longrightarrow R.$$ as a group under composition

- Group actions: ~~when R is a finite set~~, a group action of a group G on R is a group homomorphism $G \to \mathrm{Perm}(R)$.

so associated to each $g \in G$ we have a bijection φ_g on R., and $\varphi_{g_1 g_2} = \varphi_{g_1} \circ \varphi_{g_2}$

Definitions and notation.

- For a field L,

$$\mathrm{Aut}(L) = \text{the set of all field isomorphisms } L \longrightarrow L.$$

- For a field extension $K \subset L$, denote

$$\mathrm{Aut}_K(L) = \{\underline{\sigma \in \mathrm{Aut}(L)} : \underline{\sigma(k) = k, \forall\, k \in K}\} \subset Aut(L)$$

Also denote

$$\mathrm{Aut}_K(L) = \mathrm{Gal}_K(L) = \mathrm{Gal}(L/K) = \mathrm{Aut}(L/K).$$

- For non-constant $f(x) \in K[x]$ and L_f a splitting field of f over K,

$$\mathrm{Gal}_K(f) = \mathrm{Gal}(f/K) = \mathrm{Aut}_K(L_f)$$

is called the Galois group of f.

1) $\forall$ field L, $\mathrm{Aut}(L) \subset \mathrm{Perm}(L)$ is a subgroup.

2)

Lemma: For any field extenion $K \subset L$, ~~$\mathrm{Aut}(L)$ is a group and~~ $\mathrm{Aut}_K(L) \subset \mathrm{Aut}(L)$ a subgroup.

Proof. 1) If $\sigma_1, \sigma_2 : L \to L$ are isomorphism then so is $\sigma_1 \circ \sigma_2$.

2) If $\sigma_1, \sigma_2 \in \mathrm{Aut}_K(L)$, then $\forall k \in K$

$$(\sigma_1 \circ \sigma_2)(k) = \sigma_1(\sigma_2(k)) = \sigma_1(k) = k$$

So $\sigma_1 \circ \sigma_2 \in \mathrm{Aut}_K(L)$.

//

Examples. $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$ and $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{R})$.

$\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) \ni \{\mathrm{Id}_{\mathbb{C}}, \sigma\}$, where $\sigma: \mathbb{C} \to \mathbb{C}$, $\sigma(z) = \overline{z}$.

$$\left\{ \begin{array}{l} \sigma(z_1 + z_2) = \sigma(z_1) + \sigma(z_2) \\ \sigma(z_1 z_2) = \sigma(z_1)\sigma(z_2) \\ \sigma|_{\mathbb{R}} = \mathrm{id}_{\mathbb{R}} \end{array} \right\}$$

$$\sigma \circ \sigma = \mathrm{Id}_{\mathbb{C}}$$

Try: For $\alpha \in \mathbb{R}$

$$\tau(a+ib) = a + ib\alpha,$$

$$\tau(a, b) = (a, \alpha b)$$

Check: $\tau \in \mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$ iff $\alpha = \pm 1$

Claim: $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{\mathrm{Id}_{\mathbb{C}}, \sigma\}$

Side Remark: For any extension $K \subset L$, if $\sigma \in \mathrm{Aut}_K(L)$, then $\forall k \in K$, $a \in L$, $b \in L$, we must have

$$\sigma(ka) = \sigma(k)\sigma(a) = k\,\sigma(a)$$

$$\sigma(a+b) = \sigma(a) + \sigma(b)$$

Examples. $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$ ~~and $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{R})$:~~ $= \{ Id_{\mathbb{C}}, \ \sigma_0 : z \mapsto \bar{z} \}$.

Proof: Let $\sigma \in \mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$. Then

$$\sigma(a+ib) = \sigma(a) + \sigma(ib) = \sigma(a) + \sigma(i)\,\sigma(b)$$
$$= a + \sigma(i)\, b$$

But $\sigma(i) \cdot \sigma(i) = \sigma(i^2) = \sigma(-1) = -1$

So $\sigma(i) = i$ or $-i$.

Thus $\sigma = Id$ or $\sigma_0 : z \mapsto \bar{z}$.

//

Examples. $\cancel{\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})}$ ~~and~~ $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{R})$.

let $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{R})$

So $\sigma : \mathbb{R} \to \mathbb{R}$, and $\sigma(r) = r$ for all $r \in \mathbb{Q}$
bijective

and $\sigma(a+b) = \sigma(a) + \sigma(b)$, $\sigma(ab) = \sigma(a)\sigma(b)$ $\forall a, b \in \mathbb{R}$

Ex: $\sigma(a) = \begin{cases} a & \text{if } a \in \mathbb{Q} \\ 2a & \text{if } a \notin \mathbb{Q} \end{cases}$

Claim: σ must continuous. Thus $\sigma = Id_{\mathbb{R}}$

Pf: $\sigma(a^2) = \sigma(a)^2$ $\forall a \in \mathbb{R}$ $\Rightarrow$ $\sigma(a) > 0$ if $a > 0$

$\Rightarrow$ $\sigma(a) > \sigma(b)$ if $a > b$

$\sigma(a-b) = \sigma(a) - \sigma(b)$

$\Rightarrow$ If $-\frac{1}{n} < a-b < \frac{1}{n}$ $\Rightarrow$ $-\frac{1}{n} < \sigma(a) - \sigma(b) < \frac{1}{n}$

$\Rightarrow$ σ is continuous. //