Intro to Algebra 2 W5-1

fat

March 20, 2024

Corollary 1 (Corollary 28)**.** If E, E' are splitting fields for $f(x) \in F[x]$, then $\exists$ an isomorphism $\psi : E \to E'$ such that

$$\psi|_F = \mathrm{id}_F$$

Proof.

Apply theorem 27 with $F = F'$ and $\phi = \mathrm{id}_F$. ☐

Definition 1. Let F be a field. An **algebraic closure** $\bar{F}$ of F is an algebraic extension of F such that every polynomial $f(x) \in F[x]$ splits completely in $\bar{F}$. (i.e. $\bar{F}$ contains all roots of $f(x)$.)

Definition 2. A field K is **algebraically closed** if every nonconstant polynomial $f(x) \in K[x]$ splits completely in $K[x]$. (Equivalently, every polynomial $f(x) \in K[x]$ has a root in K.) ($\Leftarrow$: Let $f(x) \in K[x]$. Let $\alpha \in K$ be a root of $f(x)$ in K. Then $f(x) = (x - \alpha)g(x)$ for some $g(x) \in K[x]$. $\cdots$) (In other words, K cannot be enlarged by adding roots of $f(x) \in K[x]$.)

Example 1. $\mathbb{C}$ is algebraically closed. (Fundamental theorem of algebra)

Proposition 1 (Proposition 29)**.** Let $\bar{F}$ be an algebraic closure of F. Then $\bar{F}$ is algebraicaally closed. i.e. $\bar{\bar{F}} = \bar{F}$.

Proof.

We need to show that if $f(x) \in \bar{F}[x]$ is a nonconstant polynomial, then for a root α of $f(x)$ in $\bar{\bar{F}}$, the root must be in $\bar{F}$. By theorem 20, since $\bar{F}/F, \bar{F}(\alpha)/\bar{F}$ are both algebraic algebraic extensions, $\bar{F}(\alpha)/F$ is algebraic. In particular, α is algebraic over F. i.e. $\exists g(x) (\neq 0) \in F[x]$ such that $g(\alpha) = 0$. Since $\bar{F}$ is an algebraic closure of $F, g(x)$ splits completely over $\bar{F} \Rightarrow \alpha \in \bar{F}$. ☐

Theorem 1. Let F be a field. Then an algebraic closure of F exists. Moreover, if E, E' are 2 algebraic closures of F, then $\exists$ and isomorphism $\phi : E \to E'$ such that $\phi|_F = \mathrm{id}_F$.

Notation: We let $\bar{F}$ denote the algebraic closure of F.

13.5 Separable/Inseparable Extensions

Definition 3. Let $f(x) \in F[x]$. We say $f(x)$ is **separable** if it has no repeated roots in its splitting field. Otherwise, we say f is **inseparable**.

Example 2. (1) $f(x) = (x^2 - 2)^2 \in \mathbb{Q}[x]$ is inseparable.

(2) $F = \mathbb{F}_2(t), f(x) = x^2 - t \in F[x]$. Note that $\sqrt{t} = -\sqrt{t}$ in $F[x]$. Thus f is inseparable.

Definition 4. Let $f(x) = a_n x^n + \cdots + a_0 \in F[x]$. Then its **derivative** $\mathrm{D}f$ is defined to be

$$(\mathrm{D}f)(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$$

Lemma 1. (1) $\mathrm{D}(fg) = f\mathrm{D}g + g\mathrm{D}f$.

(2) $\mathrm{D}(cf + g) = c\mathrm{D}f + \mathrm{D}g \ \forall f, g \in F[x], c \in F$.

Proposition 2 (Propotision 33)**.** A polynomial $f(x) \in F[x]$ has a repeated root $\alpha \Leftrightarrow \alpha$ is also a root of $\mathrm{D}f$. In particular, f is separable $\Leftrightarrow \mathrm{GCD}(f, \mathrm{D}f) = 1$.

Proof.

If $\alpha \in \bar{F}$ is a repeated root of $f(x)$, then

$$f(x) = (x - \alpha)^2 g(x)$$

for some $g(x) \in \bar{F}[x]$. Now $(\mathrm{D}f)(x) = 2(x-\alpha)g(x) + (x-\alpha)^2(\mathrm{D}g)(x)$. $\Rightarrow \alpha$ is a root of $\mathrm{D}f$. Conversely assume that α is not a repeated root of $f(x)$. Then $f(x) = (x - \alpha)g(x)$ for some $g(x) \in \bar{F}[x]$ with $g(\alpha) \neq 0$. Then $(\mathrm{D}f)(x) = g(x) + (x - \alpha)(\mathrm{D}g)(x) \Rightarrow (\mathrm{D}g)(\alpha) = g(\alpha) \neq 0$. □

Example 3. $F = \mathbb{F}_2(t)$. $f(x) = x^2 - t \in F[x]$. $\mathrm{D}f = 2x = 0$. Indeeed $\sqrt{t}$ is a root of $\mathrm{D}f$.

Corollary 2 (Corollary 34)**.** Every irreducible polynomial over a field of char 0 is separable.

Proof.

Let $f(x)$ be an irreducible. Since char $F = 0$, $\deg \mathrm{D}f = \deg f - 1$. Then since f is irreducible, we must have $(f, \mathrm{D}f) = 1$. $\Rightarrow f$ is separable. □

Corollary 3. Assume char $F = p$ (p a prime). An irreducible polynomial $f(x) \in F[x]$ is inseparable $\Leftrightarrow f(x) = g(x^p)$ for some $g(x) \in F[x]$.

Proof.

If $f(x) = g(x^p)$ for some $g(x) \in F[x]$, say $g(x) = a_n x^n + \cdots + a_0$. Then

$$f(x) = a_n x^{pn} + a_{n-1}x^{p(n-1)} + \cdots + a_1 x^p + a_0$$

$$\mathrm{D}f(x) = pna_n x^{pn-1} + \cdots + pa_1 x^{p-1} = 0$$

$\Rightarrow (f, \mathrm{D}f) = f \neq 1$. By prop 33, f is inseparable.

Conversely if $f(x)$ is not of the form $g(x^p)$, i.e. $f(x) = b_n x^n + \cdots + b_0$ with $b_j \neq 0$ for some j with $p \not| j$.

$$\Rightarrow \mathrm{D}f = \cdots + jb_j x^{j-1} + \cdots \neq 0$$

$$\Rightarrow (f, \mathrm{D}f) = 1$$

$\Rightarrow f$ is separable. □

We next show that if F is a finite field of char p then every polynomial of the form $g(x^p)$ is reducible. Thus, according to the corollary above, every irreducible polynomial over a finite field is separable.

Example 4. We have seen that $x^2 - t \in \mathbb{F}_2(t)[x]$ is inseparable. It is irreducible. This could happen because $\mathbb{F}_2(t)$ is an infinite field of char $\neq 0$.

Proposition 3 (Proposition 35)**.** Assume that char $F = p$. Then $\forall a, b \in F$,

$$(a+b)^p = a^p + b^p$$

$$(ab)^p = a^p b^p$$

i.e. the function $a \mapsto a^p$ is an injective homomorphism from F to F.

Proof.

$$(ab)^p = a^p b^p$$

is clear. Now

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \cdots + \binom{p}{p-1} a b^{p-1} + b^p$$

Observe that $p | \binom{p}{j}$ for $j = 1, ..., p-1$. $\Rightarrow (a+b)^p = a^p + b^p$. □

Corollary 4 (Corollary 36)**.** If F is a finite field of char p, then $a \mapsto a^p$ is an automorphism of F.

Proof. Since F is a finite field, any injective homorphism is an automorphism. □

Definition 5. The function $a \mapsto a^p$ is called the **Frobenius endomorphism**. (or **Frobenius automorphism** when it is an isomorphism.)

Example 5. For an infinite field of char p, the function $a \mapsto a^p$ may not be surjective. For example, $K = \mathbb{F}_2(\sqrt{t})$.

Claim. The image of the Frob. endo. is $\mathbb{F}_2(t)$, a proper subfield of K.

Proof.

Say

$$r = \frac{a_n(\sqrt{t})^n + \cdots + a_0}{b_n(\sqrt{t})^n + \cdots + b_0} \in K$$

Then

$$r^2 = \frac{\left(a_n(\sqrt{t})^n + \cdots + a_0\right)^2}{\left(b_n(\sqrt{t})^n + \cdots + b_0\right)^2} = \frac{a_n^2 t^n + \cdots + a_0^2}{b_n^2 t^n + \cdots + b_0^2} \in \mathbb{F}_2(t)$$

□

Proposition 4 (Proposition 37)**.** Every irreducible polynomial over a finite field F is separable.

Proof.

Assume that char $F = p$ and $f(x)$ is an irreducible polynomial in $F[x]$. Assume that $f(x)$ is inseparable. By Corollary (the one after corollary 34), $f(x) = g(x^p)$ for some $g(x) \in F[x]$. Say $g(x) = a_n x^n + \cdots + a_0$. Now by corollary 36, $a \mapsto a^p$ is surjective. Thus $\forall j, \exists b_j \in F$ such that $b_j^p = a_j$. Then

$$f(x) = a_n x^{pn} + \cdots + a_0 = b_n^p x^{pn} + \cdots + b_0^p$$

$$= (b_n x^n + \cdots + b_0)^p$$

which is not an irreducible, a contradiction. Thus f is separable. $\square$