MA542 Lecture

Timothy Kohl

Boston University

March 17, 2025

Splitting field of $x^n - a$

Last time, we saw that for a field $F[x]$ and an irreducible polynomial $p(x) \in F[x]$ that any two splitting fields for $p(x)$ over F are isomorphic.

As a small generalization of the earlier example, let's determine the splitting field for $x^n - a \in \mathbb{Q}[x]$ where $a \in \mathbb{Q}$ is not an n^{th} power of any other rational number.

As such, $a^{1/n}$ is an irrational value that is one of the roots of $x^n - a$, and the totality of them is

$$\{a^{1/n}, \zeta a^{1/n}, \zeta^2 a^{1/n}, \ldots, \zeta^{n-1} a^{1/n}\}$$

where $\zeta = e^{\frac{2\pi i}{n}}$ is a primitive n^{th} root of unity, namely the principal solution of $x^n - 1$.

As to a (really the) splitting field $E/\mathbb{Q}$, we again observe that $a^{1/n} \in E$ and also $\zeta a^{1/n}$ which means $\frac{\zeta a^{1/n}}{a^{1/n}} = \zeta \in E$, and so E contains $\mathbb{Q}(\zeta)$ and $\mathbb{Q}(a^{1/n})$ and so $E = \mathbb{Q}(\zeta, a^{1/n})$.

As we observed earlier, for $n = 3$, $\mathbb{Q}(\zeta) = \{a + b\zeta \mid a, b \in \mathbb{Q}\}$ since $\zeta^2 + \zeta + 1 = 0$, and so $dim_{\mathbb{Q}}(\mathbb{Q}(\zeta, a^{1/3})) = dim_{\mathbb{Q}}(\mathbb{Q}(\zeta)) \cdot dim_{\mathbb{Q}}(\mathbb{Q}(a^{1/3})$.

For general n we still have $dim_{\mathbb{Q}}(\mathbb{Q}(\zeta, a^{1/n})) = dim_{\mathbb{Q}}(\mathbb{Q}(\zeta)) \cdot dim_{\mathbb{Q}}(\mathbb{Q}(a^{1/n}))$ but the question is, what is $dim_{\mathbb{Q}}(\mathbb{Q}(\zeta))$?

As it turns out $dim_{\mathbb{Q}}(\mathbb{Q}(\zeta)) = \phi(n)$ where ϕ is the Euler function, specifically $\phi(n) = |U(\mathbb{Z}_n)| = |\{r \in \mathbb{Z}_n \mid gcd(r, n) = 1\}|$.

(more on this later)

Zeros

We now wish to consider the following question: For a field F, and $p(x) \in F[x]$ irreducible, how many *distinct* roots does $p(x)$ have in its splitting field?

More pointedly, does $p(x)$ ever have *repeated* roots?

Definition

Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$ for F a field. The *derivative* (yes derivative!) of $f(x)$ is the polynomial
$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + a_1 \in F[x]$

Here we use this definition of derivative to utilize the algebraic relationship(s) that exist between $f(x)$ and $f'(x)$ and are not, in any way, doing calculus.

Lemma

Let $f(x), g(x) \in F[x]$ and $a \in F$ then
(a) $(f+g)' = f' + g'$
(b) $(af)' = af'$
(c) $(fg)' = f'g + fg'$

In particular we are interested in the relationship between the roots of $f(x)$ and those of $f'(x)$.

One thing to note is the distinction between $f(x)$ and $f'(x)$ when $char(F) = 0$ versus when $char(F) = p$ for p a prime.

If $deg(f(x)) = n$ then

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$
$$\downarrow$$
$$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + a_1$$

and so $deg(f'(x)) = n - 1$, *unless* $n a_n = 0$.

Since $a_n \neq 0$ then $n a_n = 0$ implies $n = 0$, but if $char(F) = 0$ and $deg(f(x)) \geq 1$ then this is impossible.

However, if $char(F) = p$ then it is possible for $f'(x) = 0$, even though $f(x) \neq 0$.

This would imply that $ka_k = 0$ for each k from 1 to n.

Lemma

If $f(x) \in F[x]$ is a non-zero polynomial, where $char(F) = p$, then $f'(x) = 0$ if and only if $f(x) = g(x^p)$ for some polynomial $g(x)$.

We note that if $f(x) = g(x^p)$ for some polynomial $g(x)$ then the only powers of x that appear in $f(x)$ are multiples of p.

So if, e.g.

$$g(x) = x^3 + 2x^2 - 5x - 2$$

then for

$$\begin{aligned} f(x) = g(x^p) &= (x^p)^3 + 2(x^p)^2 - 5(x^p) - 2 \\ &= x^{3p} + 2x^{2p} - 5x^p - 2 \end{aligned}$$

we have that

$$f'(x) = 3px^{3p-1} + 2(2p)x^{2p-1} - 5px^{p-1} = 0$$

.

Theorem

If F is a field and $f(x) \in F[x]$ is a non-constant polynomial then
(a) if $f'(x) = 0$ then every root of $f(x)$ is a repeated root
(b) if $f'(x) \neq 0$ then $f(x)$ has multiple zeros in some extension field E/F if and only if $f(x)$ and $f'(x)$ have a common factor of positive degree in $E[x]$.

PROOF: For part (a) suppose $f'(x) = 0$.

If $f(x) = (x - \alpha)g(x)$ then $f'(x) = g(x) + (x - \alpha)g'(x)$ and so $f'(x) = 0$ implies

$$g(x) = -(x - \alpha)g'(x)$$

and so $f(x) = -(x - \alpha)^2 g'(x)$ and since $f(x) \neq 0$ then $g'(x) \neq 0$ and so $f(x)$ has a repeated root.

i.e. *Any* root α of $f(x)$ is a repeated root and $(x - \alpha)$ is automatically a divisor of $f(x)$ and (vacuously) $f'(x)$ (since 0 is divisible by every polynomial!)

Now $f(x)$ having a multiple zero $\alpha \in E$ means that in $E[x]$, $f(x) = (x - \alpha)^2 g(x)$ for some polynomial $g(x)$.

So by the product rule, $f'(x) = 2(x - \alpha)g(x) + (x - \alpha)^2 g'(x)$ which means $(x - \alpha) \mid f'(x)$ where, also, by assumption $(x - \alpha) \mid f(x)$ already. (i.e. f and f' have a common factor of degree ≥ 1)

PROOF (continued)
If $f(x)$ and $f'(x)$ have a common divisor $g(x)$ of positive degree, then a root α of $g(x)$ is a root of $f(x)$ and $f'(x)$ so

$$f(x) = (x-\alpha)h(x)$$
$$\downarrow$$
$$f'(x) = h(x) + (x-\alpha)h'(x)$$

and so $f'(\alpha) = h(\alpha) = 0$ but this means $h(x) = (x-\alpha)k(x)$ and therefore $f(x) = (x-\alpha)^2 k(x)$ and so $f(x)$ has a repeated root. $\square$.

Theorem

Let F be a field and let $f(x) \in F[x]$ be irreducible. If $char(F) = 0$ then $f(x)$ has no repeated roots in any splitting field. If $char(F) = p$ for $p \neq 0$ (i.e. p prime) then $f(x)$ has a multiple zero only if it is of the form $f(x) = g(x^p)$ for some $g(x) \in F[x]$.

PROOF: Since $f(x)$ is irreducible, then $f(x)$ is non-constant.

If $f'(x) = 0$ then we must have $char(F) = p$ and that $f(x) = g(x^p)$ and, moreover that every root of $f(x)$ is a repeated root.

Suppose now that $char(F) = 0$. If $f(x)$ has multiple zeros then $f(x)$ and $f'(x)$ have a common factor $g(x)$ where $deg(g(x)) \geq 1$.

So $g(x) \mid f(x)$ and $g(x) \mid f'(x)$. However, since $deg(f'(x)) < deg(f(x))$ then $deg(g(x)) \leq deg(f'(x)) < deg(f(x))$ which means $g(x)$ is a factor of the presumably irreducible polynomial $f(x)$, of lower degree than $deg(f(x))$ which is impossible. □

Definition

A polynomial $f(x) \in F[x]$ is separable if $f(x)$ has no repeated roots.

So we've seen then that if $char(F) = 0$ then all irreducible polynomials are separable.

So what about the case when $char(F) = p$?

Definition

A field F is called perfect if either $char(F) = 0$ or, if $char(F) = p$ that $F^p = \{a^p \mid a \in F\} = F$.

Theorem

Finite fields are perfect.

Proof.

For a finite field F, we have that $char(F) = p$ for some prime p.
Define $\phi : F \to F$ by $\phi(a) = a^p$, and observe that
$\phi(ab) = (ab)^p = a^p b^p = \phi(a)\phi(b)$.
Also, $\phi(a + b) = (a + b)^p = a^p + b^p$ (exercise) and so ϕ is a homomorphism of rings.
Note also that if $\phi(a) = 0$ then $a^p = 0$, but since F is a field, and therefore a domain, we have $a = 0$.
This means that $Ker(\phi) = \{0\}$ which means ϕ is 1-1.
So now $\phi : F \to F$ is a function from a finite set to itself that is injective, so it must be surjective (onto) as well. Thus $\phi(F) = F^p = F$. □

Theorem

If F is a perfect field then all irreducible polynomials in $F[x]$ are separable.

Proof.

We already know that the statement is true when $char(F) = 0$, so suppose $char(F) = p$.
If $f(x) \in F[x]$ is irreducible then either $f'(x) = 0$ or $f'(x) \neq 0$.
If $f'(x) \neq 0$ then it has no repeated roots.
If $f'(x) = 0$ then $f(x) = g(x^p)$ for some $g(x)$.
If $g(x) = a_n x^n + \cdots + a_1 x + a_0$ then $g(x^p) = a_n x^{pn} + a_{n-1} x^{p(n-1)} + \cdots + a_1 x^p + a_0$
but now, since F is perfect, then for each i, $a_i = b_i^p$ for some $b_i \in F$.

But then we have that

$$\begin{aligned} f(x) = g(x^p) &= a_n x^{pn} + a_{n-1} x^{p(n-1)} + \cdots + a_1 x^p + a_0 \\ &= b_n^p x^{pn} + b_{n-1}^p x^{p(n-1)} + \cdots + b_1^p x^p + b_0^p \\ &= (b_n x^n + \cdots + b_1 x + b_0)^p \end{aligned}$$

and so $f(x)$ is not irreducible. □