MA542 Lecture

Timothy Kohl

Boston University

March 19, 2025

Last time, we showed that if F is a perfect field then all irreducible polynomials in $F[x]$ are separable.

Recall that F is a perfect field if $char(F) = 0$ or, if $char(F) = p$ that $F^p = F$.

Perfect or not, we can say something quite general about the multiplicities of roots of irreducible polynomials in $F[x]$.

Theorem

Let $f(x)$ be irreducible in $F[x]$ for F a field, and let E be a splitting field for $f(x)$ over F. Then all the zeros of $f(x)$ in E have the same multiplicity.

PROOF:

If a and b are roots of $f(x)$ in a splitting field E/F of $f(x)$, then there is an isomorphism $\psi : F(a) \to F(b)$, induced by $\psi(a) = b$ and $\psi(c) = c$ for $c \in F$, so, in particular $\psi(c_{n-1}a^{n-1} + \cdots + c_1 a + c_0) =$ $c_{n-1}\psi(a^{n-1}) + \cdots + c_1\psi(a) + c_0 = c_{n-1}b^{n-1} + \cdots + c_1 b + c_0$ where $c_i \in F$.

So if a has multiplicity m then $f(x) = (x-a)^m g(x) \in E[x]$ (where $g(a) \neq 0$) and $\psi(f(x)) = (x - \psi(a))^m \psi(g(x)) = (x-b)^m \psi(g(x))$ which means b has multiplicity *at least* m but if we exchange 'a' and 'b' then we deduce that the multiplicity of a is greater than or equal to that of a as well, so they're the same. □

So we conclude that $f(x) = c(x - a_1)^m(x - a_2)^m \cdots (x - a_r)^m$ for some $c \in F$ where $a_1, \ldots, a_r$ are the distinct roots of $f(x)$.

We finish by considering a 'non-perfect' field.

Consider $\mathbb{Z}_p(t) = Frac(\mathbb{Z}_p[t])$ which is the field of fractions where numerator and denominator are polynomials in 't' with coefficients in $\mathbb{Z}_p$, what we term a 'field of rational functions'.

What we find is that the function $\phi : \mathbb{Z}_p(t) \to \mathbb{Z}_p(t)$ given $\frac{f(t)}{g(t)} \mapsto \frac{f(t)^p}{g(t)^p}$ is not onto.

To see this, realize that $\phi(t) = t^p$ which means $t \notin \phi(\mathbb{Z}_p(t))$ since t is not the p^{th} power of any element of $\mathbb{Z}_p(t)$.

Now $f(x) = x^p - t \in \mathbb{Z}_p(t)[x]$ is an irreducible polynomial, basically since $\mathbb{Z}_p(t)$ does not contain $t^{1/p}$.

So now, if $s = t^{1/p}$ then we can adjoin s to $\mathbb{Z}_p(t)$ to obtain an extension field and in this field $(x - s)^p = x^p - s^p = x^p - t$ since the field has characteristic p.

So we conclude that $f(x) = x^p - t$ is an irreducible polynomial that is not separable.

Algebraic Extensions

Definition

Let E be an extension field of F and let $a \in E$. We call a algebraic over F if a is the zero of some non-zero polynomial in $F[x]$.

If 'a' is not algebraic, then it is called transcendental.

An extension E of a field F is called algebraic if every element of E is algebraic over F, otherwise E is a transcendental extension of F.

An extension of F of the form $F(a)$ is called a simple extension.

Examples:
$\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ is algebraic over $\mathbb{Q}$ since $\sqrt{2}$ is a root of $x^2 - 2 \in \mathbb{Q}[x]$.

The field $\mathbb{Q}(\sqrt{2})$ is algebraic, and we can show this by looking at a typical element $\alpha = a + b\sqrt{2}$.

If $b = 0$ then $\alpha = a \in \mathbb{Q}$ which is root of $x - a \in \mathbb{Q}[x]$ (indeed all the elements of F are algebraic over F for any field).

If $b \neq 0$ then consider $\alpha - a = b\sqrt{2}$ so $(\alpha - a)^2 = 2b^2$ so α is a root of $f(x) = x^2 - 2ax + (a^2 - 2b) \in \mathbb{Q}[x]$.

In contrast, π is transcendental over $\mathbb{Q}$, as was proved by Lindemann in 1882.

Similarly e is also known to be transcendental, as was proved by Hermite in 1873.

As is turns out, it's rather difficult to prove a number is transcendental.

Another famous example is the so-called Liouville constant:

$$L = \sum_{n=1}^{\infty} 10^{-n!} = 10^{-1} + 10^{-2} + 10^{-6} + \cdots = 0.110001000...$$

where a given digit is 1 if its 'place' is $n!$ for some $n \geq 1$.

For perspective, we can consider the fact that the set of all real numbers which are alebraic over $\mathbb{Q}$, namely the roots of any polynomial in $\mathbb{Q}[x]$ is a countable set since there are only countably many polynomials in $\mathbb{Q}[x]$, each of which has only finitely many roots.

The difference of these two sets is uncountable, meaning that **most** real numbers are transcendental but the subtlety is in actually *proving* a given real number is transcendental.

If we take a transcendental number like say π then $\mathbb{Q}(\pi)$ contains all possible $\mathbb{Q}$-linear combinations of powers of π, i.e $f(\pi)$ where $f(x) \in \mathbb{Q}[x]$.

The key difference between $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\pi)$ is that π is not the root of a polynomial, unlike $\sqrt{2}$, and the difference is that $\mathbb{Q}(\pi)$ is not a finite dimensional vector space over $\mathbb{Q}$.

(i.e. $\sqrt{2}$ being a root of $x^2 - 2$ means all elements of $\mathbb{Q}(\sqrt{2})$ are of the form $a + b\sqrt{2}$, but the same is not true for $\mathbb{Q}(\pi)$)

Indeed $\mathbb{Q}(\pi) = \left\{ \frac{f(\pi)}{g(\pi)} \mid f(x), g(x) \in \mathbb{Q}[x], g(x) \neq 0 \right\}$ namely all rational functions with π substituted in for x.

For any field F, we have $F(t) = Frac(F[t])$ which is the field of rational functions in one variable 't' with coefficients in F.

We see that $F(t)$ is a transcendental extension of F since there is no polynomial $f(x) \in F[x]$ such that $f(t) = 0$.

Theorem

For a field F, and a a transcendental element over F we have that $F(a) \cong F(t)$.
If α is algebraic over F then $F(\alpha) \cong F[x]/\langle p(x)\rangle$ for an irreducible polynomial $p(x) \in F[x]$ of minimal degree for which $p(\alpha) = 0$.

We examine the second claim above.

If α is algebraic over F then consider

$$I = \{f(x) \in F[x] \mid f(\alpha) = 0\}$$

and observe that $f(x), g(x) \in I$ implies $f(x) + g(x) \in I$ too since $f(\alpha) + g(\alpha) = 0 + 0 = 0$ and if $h(x) \in F[x]$ and $f(x) \in I$ then for $f(x)h(x)$ we have $f(\alpha)h(\alpha) = 0h(\alpha) = 0$ so $h(x)f(x) \in I$, that is, I is an ideal.

And being an ideal in $F[x]$, it is principal so it means that $I = \langle p(x) \rangle$ for some $p(x) \in F[x]$, and moreover since the degrees of elements in I are natural numbers, the degree of $p(x)$ is the minimal degree of the degrees of all the elements of I.

It follows that $p(x)$ must be irreducible. Why?

Define $\psi : F[x]/I \to F(\alpha)$ by $h(x) + I \mapsto h(\alpha)$ and if $h_1(x) + I = h_2(x) + I$ then $h_1(x) - h_2(x) \in I$ and so $h_1(\alpha) - h_2(\alpha) = 0$ which means $h_1(\alpha) = h_2(\alpha)$ so ψ is well defined, and a homomorphism.

It is clear that ψ is onto since every element of $F(\alpha)$ is of the form $h(\alpha)$ for some $h(x) \in F[x]$ and as we saw above $h_1(\alpha) = h_2(\alpha)$ implies $h_1(x) + I = h_2(x) + I$ so ψ is one-to-one and so $F[x]/I \cong F(\alpha)$ which means that I is a maximal ideal.

As such, for that $p(x)$ such that $I = \langle p(x) \rangle$ we must have that $p(x)$ is irreducible.

The reason is that if $q(x) \mid p(x)$ (where $deg(q(x)) < deg(p(x))$) then $\langle p(x) \rangle \subsetneq \langle q(x) \rangle$ but since $\langle p(x) \rangle$ is maximal this means $\langle q(x) \rangle = F[x]$ so that $q(x)$ is a non-zero constant (i.e. a unit). □

We have the following somewhat refined version of the above result.

Theorem

If α is algebraic over F then there is a unique monic (leading term 1) irreducible polynomial $p(x) \in F[x]$ such that $p(\alpha) = 0$.

The ideal I of polynomials in $F[x]$ which have α as a root are generated by an irreducible polynomial, i.e. $I = \langle p(x) \rangle$.

And any other polynomial which generates this ideal is a unit multiple of $p(x)$, so if $p(x) = a_n x^n + \cdots + a_1 x + a_0$ then $up(x) = ua_n x^n + ua_{n-1} x^{n-1} + \cdots + ua_1 + ua_0$ and so $up(x)$ is monic only if $u = a_n^{-1}$ i.e. it's unique.

We call this unique monic irreducible polynomial the *minimal polynomial* of α over F and denote it $irr(\alpha, F)$.

The assumptions we will make about the fields under study make the following definitions from the text somewhat moot, be we include them nonetheless.

Definition

For a field F, an extension field E/F is called a separable extension if for every $\alpha \in E$, one has that $irr(\alpha, F)$ is a separable polynomial.
An extension E/F is a normal extension if E is a separable splitting field of some polynomial in $F[x]$.

These definitions are made if one makes **no** assumptions about the base field F.

However, if F is perfect (which we shall usually assume) then any extension field E/F is automatically separable.

And as to normal extensions, again assuming the base field F is perfect, then 'normal extension' is equivalent to 'splitting field'.

And indeed, we shall have good reasons for distinguishing between splitting fields/extensions, such as $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, versus those which aren't such as $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.

Here are some basic examples of $irr(\alpha, \mathbb{Q})$.

- $\alpha = \sqrt{2}$ implies $irr(\alpha, \mathbb{Q}) = x^2 - 2$
- $\alpha = i$ implies $irr(\alpha, \mathbb{Q}) = x^2 + 1$
- $\alpha = \sqrt[3]{2}$ implies $irr(\alpha, \mathbb{Q}) = x^3 - 2$

These are relatively obvious, but what about more complicated examples?

We'll consider these next time, as the problem is in *proving* that the polynomial you find is actually irreducible.