Modern Algebra Lecture Notes: Rings and fields set 8, revision 3

Kevin Broughan

University of Waikato, Hamilton, New Zealand

May 25, 2010

Extension fields, splitting fields

Definitions

A field E is called an extension field of a field F if $F \subset E$ and F is a subfield of E.
If $F \subset E$ and E is an extension field of F and a polynomial $f(x) \in F[x]$ factors completely into linear factors in E (we say then that $f(x)$ **splits** in E), but does not split in any proper subfield of E, we say E is a splitting field for $f(x)$ over F.

Examples

(1) $f(x) = (x-1)(x-2)(x-3)$ in $\mathbb{Q}[x]$ splits in $E = F = \mathbb{Q}$ which has no subfields, so $\mathbb{Q}$ is the splitting field.

(2) $g(x) = x^2 - 2$ is in $\mathbb{Q}[x]$ and splits in $\mathbb{C}$ which is a field extension of $F = \mathbb{Q}$, but it also splits in $E = Q(\sqrt{2}) = \{a + \sqrt{2}b : a, b \in \mathbb{Q}\}$, which is a smaller extension of $\mathbb{Q}$. Thus $\mathbb{C}$ is not the splitting field of $g(x)$. In E, $g(x) = (x + \sqrt{2})(x - \sqrt{2})$.

(3) $h(x) = x^n - 1 = (x-1)(x-\omega)((x-\omega^2)\cdots(x-\omega^{n-1})$, where $\omega = e^{\frac{2\pi i}{n}}$ is the fundamental primitive n'th root of unity. Then the splitting field of $h(x)$ is $\mathbb{Q}(\omega)$.

Statement

Let $f(x) \in F[x]$ be of $\deg f(x) > 0$. Then there is an extension E of F in which $f(x)$ has a root.

Proof

Let $E = F[x]/\langle f(x) \rangle$. Then, since $f(x)$ is irreducible, E is a field. The mapping $\theta : F \to E$ defined by the rule $b \to [b]$ is an injective homomorphism, so we can regard F as a subfield of E and $f(x)$ as having coefficients in this subfield.

Then in E, let $a = [x]$ and then $f(a) = f([x]) = [f(x)] = [0] = 0$ where the last 0 is the 0 of E. Therefore $f(x)$ has a zero in E.

Definition

Let E be an extension of F and let $0 \neq a \in E$ be an element. We define $F(a)$ to be the smallest subfield of E containing a. Note that it must also contain $2a, 3a, -a, 1/a, a^2, g(a)/h(a), \ldots$ where $g(x), h(x) \in F[x]$ and $h(a) \neq 0$ in E.

Examples of $F(a)$

1. $\mathbb{Q}(2) = \mathbb{Q}$.
2. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.
3. If x is an indeterminant, $\mathbb{Q}(x) = \{f(x)/g(x) : f(x),\ g(x) \in \mathbb{Q}[x],\ g(x) \neq 0\}$ i.e. $g(x)$ is not the zero polynomial.
4. $\mathbb{Q}(\pi) = \{f(\pi)/g(\pi) : f(x),\ g(x) \in \mathbb{Q}[x],\ g(x) \neq 0\}$.

Extended definitions

If $a, b, a_i \in E$, and extension of F, We can define $F(a, b)$ by $(F(a))(b)$ and inductively $F(a_1, \ldots, a_n) = (F(a_1, \ldots, a_{n-1}))(a_n)$, or simply as the smallest subfield of E containing all of the a, b, a_i.

Splitting fields exist: Theorem 31

Statement

Let $f(x) \in F[x]$ be of $\deg f(x) > 0$. Then there is an extension E of F which is a splitting field for $f(x)$. All splitting fields are isomorphic, so this field is essentially unique. The proof is omitted.

Fundamental Theorem of Algebra

The $\star$ Fundamental Theorem of Algebra $\star$, proved in Complex Calculus, shows that every polynomial with complex coefficients has a full set of roots in $\mathbb{C}$. Thus if $F = \mathbb{Q}$, there is at least one field extension of $\mathbb{Q}$ in which $f(x)$ splits completely. Later we will have an algebraic proof, which relies on the existence of a splitting field for each polynomial over a given field.

Dangerous curve!

Splitting fields can be of large dimension. There are examples of irreducible polynomials $f(x) \in \mathbb{Q}[x]$ with degree n and splitting fields of maximum dimension $n!$.

A splitting field of maximum dimension

This is somewhat more than what we have been doing, but for those interested:

(1) Let $x_1, \cdots, x_n$ be indeterminants, F a given field and $R = F(x_1, \ldots, x_n)$ the field of rational functions in those indeterminants. Let S be the subfield of symmetric rational functions $s_1, \ldots, s_n$ in the indeterminants $x_1, \ldots, x_n$. For example $s_1 = x_1 + x_2 + \cdots + x_n$ and $s_n = x_1 \cdots x_n$. Then $S = F(s_1, \ldots, s_n)$.

(2) Let $f(x) = x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n$. Then R is the splitting field of $f(x)$ over S and $[R : S] = n!$.

Differential algebra: derivative of a polynomial

Definition

Let $f(x) \in F[x]$ be a polynomial $f(x) = a_0 + \cdots a_n x^n$. Then if $n = 0$ set $f'(x) = 0$. Otherwise define

$$f'(x) := a_1 + 2a_2 x + 3a_3 x^2 \cdots + n a_n x^{n-1},$$

and call $f'(x)$ the derivative of $f(x)$. We sometimes write $(f(x))'$ for $f'(x)$.

Theorem 32: Properties of the derivative

Let $f(x), g(x) \in F[x]$ and $a \in F$. Then
(1) $(f(x) + g(x))' = f'(x) + g'(x)$,
(2) $(af(x))' = af'(x)$,
(3) $(f(x).g(x))' = f(x).g'(x) + f'(x).g(x)$.

Proof of (1)

$$\begin{aligned} f(x) &:= a_0 + a_1 x + \cdots + a_n x^n,\ g(x) := b_0 + b_1 x + \cdots + b_n x^n \\ (f(x) + g(x))' &= (a_1 + b_1) + (a_2 + b_2)x + \cdots + n(a_n + b_n)x^{n-1} \\ &= (a_1 + \cdots + n a_n x^{n-1}) + (b_1 + \cdots + n b_n x^{n-1}) \\ &= f'(x) + g'(x) \end{aligned}$$

Proof of (2)

$$(af(x))' = \sum_{j=1}^{n} jaa_j x^{j-1} = a(\sum_{j=1}^{n} ja_j x^{j-1}) = af'(x)$$

Proof of (3): derivative of a product

First prove (3) for monomials:

$$\begin{aligned}
f(x) &:= a_n x^n,\ n \geq 1 \\
(f(x).g(x))' &= (\sum_{j=0}^{m} a_n b_j x^{n+j})' \\
&= \sum_{j=0}^{m} (n+j) a_n b_j x^{n+j-1} \\
&= \sum_{j=0}^{m} n a_n x^{n-1} b_j x^j + \sum_{j=1}^{m} a_n x^n j b_j x^{j-1} \\
&= f'(x).g(x) + f(x).g'(x).
\end{aligned}$$

Then complete the proof using linearity (1) and (2).

Example

Let $f(x) = x^4 + x^2 + 1 \in \mathbb{Z}/2\mathbb{Z}$. Then $f'(x) = 0$ but $f(x)$ is **not** the constant polynomial.

In characteristic zero, $f'(x) = 0 \implies f(x) = a_0 \in F$, a constant. In characteristic p, $f'(x) = 0 \implies f(x) = g(x^p)$.

The chain rule makes sense: $f(g(x))' = f'(g(x).g'(x)$, but to discuss the quotient rule we need rational functions, which are outside our scope.

Derivations

This derivative is called a derivation. Are their other derivations ?

Multiple zero criterion

Examples

$f(x) = 1 + 2x + x^2,\ f'(x) = 2 + 2x$ so in $\mathbb{Q}[x]$,
$(f(x), f'(x)) = (2(1 + x), (1 + x)^2) = 1 + x \neq 1$ and $f(x)$ has a multiple zero, -1, in $\mathbb{Q}$.
$f(x) = 1 + x + x^2,\ f'(x) = 1 + 2x$ so $(f(x), f'(x)) = (1 + x + x^2, 1 + 2x) = 1$ in $\mathbb{Q}[x]$ so in any extension $f(x)$ has only simple zeros.

Theorem 33:

The polynomial $f(x) \in F[x]$ has a multiple zero in some extension of F if and only if $f(x)$ and $f'(x))$ have a non-trivial common divisor of positive degree in $F[x]$, so the GCD $(f(x), f'(x))$ is non-trivial in $F[x]$

proof

First let $f(x)$ have a multiple zero $a \in E$. Then
$f(x) = (x - a)^2 g(x)$ thus

$$f'(x) = 2(x - a)g(x) + (x - a)^2 g'(x) = (x - a)(2g(x) + (x - a)g'(x).$$

Since $x - a \mid (f(x), f'(x))$ it is a common divisor of positive degree in $E[x]$.

Multiple zero criterion completed

Key step

If the GCD $(f(x), f'(x)) = 1$ in $F[x]$, then via the Euclidean algorithm we can find polynomials $u(x),\ v(x) \in F[x]$ such that $u(x)f(x) + v(x)f'(x) = 1$. But viewing this as an equation in $E[x]$ we get $x - a \mid 1$, which is impossible. Therefore the GCD is non-trivial in $F[x]$.

If the GCD $g(x)$ is non-trivial, let E be an extension in which this GCD has a zero, and let $a \in E$ be one of those zeros, so $g(a) = 0$. Then $f(a) = f'(a) = 0$ in $E[x]$. Hence $f(x) = (x - a)q(x)$ so $f'(x) = q(x) + (x - a)q'(x)$. Letting $x = a$ we get $0 = f'(a) = q(a)$ and thus $q(x) = (x - a)p(x)$ and so $f(x) = (x - a)^2 p(x)$ and we have shown $f(x)$ has a multiple root.$\square$

Irreducibles have only simple zeros in characteristic zero

Theorem 34:

Let $f(x) \in F[x]$ be irreducible, where F has characteristic zero. Then in any extension field, $f(x)$ has no multiple zeros.

proof

We use Theorem 33. If $f(x)$ has a multiple zero in some extension field of F then the GCD $(f(x), f'(x))$ is non-trivial in $F[x]$. But $f(x)$ is irreducible, therefore $f(x) \mid f'(x)$.

Since when $f'(x) \neq 0$ this means $\deg f(x) \leq \deg f'(x)$, which is impossible, we must have $f'(x) = 0$.

But if $f(x) = a_0 + \cdots + a_n x^n,\ n \geq 1,\ a_n \neq 0$, we must have $0 = f'(x) = \cdots n a_n x^{n-1}$ so $n a_n = 0$, which in characteristic zero is impossible. Therefore all zeros in all extension fields of the irreducible $f(x)$ must be simple. $\square$

Theorem 35:⋆ $F(a) \approx F[x]/\langle f(x)\rangle$ ⋆

Recall $F(a)$

Let $F \subset E$ with E an extension field of F and $a \in E$. Then we define $F(a)$ to be the smallest subfield of E which contains both F and a.

Statement

Let $f(x) \in F[x]$ be irreducible and $f(a) = 0$ in E. Then

(1) The field $F(a)$ is isomorphic to the field $F[x]/\langle f(x)\rangle$.

(2) If $\deg f(x) = n$ then $F(a)$ is a vector space over F with basis $\{1, a, a^2, \ldots, a^{n-1}\}$.

(3) If $a' \in E'$ is another zero of $f(x)$ then $F(a) \approx F(a')$.

Proof of (1)

Define $\theta : F[x] \to E$ by $\theta(h(x)) = h(a)$. Then, since $f(a) = 0$, we can show $\ker\theta = \langle f(x)\rangle$. Firstly
$h(x) = g(x).f(x) \in \langle f(x)\rangle \implies \theta(g(x).f(x)) = g(a).f(a) = 0$, so $h(x) \in \ker\theta$ and we thus have $\langle f(x)\rangle \subset \ker\theta$. But since $\theta(1) = 1 \neq 0$, $\ker\theta \neq F[x]$. And since $f(x)$ is irreducible, $\langle f(x)\rangle$ is a maximal ideal, so therefore $\langle f(x)\rangle = \ker\theta$.

Now we simply use the isomorphism theorem for rings to get

$$F[x]/\langle f(x)\rangle \approx \theta(F[x]) \subset E$$

i.e. isomorphic as fields, so all we need do is identify the range of θ.

Let $a_0 \in F$. Then the constant polynomial with value a_0 is mapped by θ to a_0 so we get all of F in the range. The polynomial $g(x) = x$ is mapped to a, so we get that as well. Since the image of generic polynomial (we write a_i for $[a_i]$ since the class is unique for each $a_i \in F$), $g(x) = a_0 + a_1 x + \cdots + a_m x^m$ is $g(a) = a_0 + a_1 a + \cdots + a_m a^m$, and the image is a field, all be need is the field generated by F and a in E, i.e. $F(a)$.

Proof of (2)

Let $\deg f(x) = n \geq 1$. Then, working in $F[x]/\langle f(x)\rangle$, we can write $g(x) = f(x)q(x) + r(x)$ so $g(x) - r(x) \in \ker\theta$, $[g(x)] = [r(x)]$ and $\theta(g(x)) = g(a) = r(a)$. Therefore every element of $F(a)$ can be expressed as $r(a) = a_0 + a_1 a + \cdots a_{n-1} a^{n-1}$.

This expression for $r(a)$ is unique, so therefore the set $\{1, a, a^2, \ldots, a^{n-1}\}$ is linearly independent and spans $F(a)$ which is thus a vector space of dimension $[F(a) : F] = n$.

Proof of (3)

Let $a \in E,\ b \in K$ be zeros of $f(x)$. Then

$$F(a) \approx F[x]/\langle f(x)\rangle \approx F(b) \implies F(a) \approx F(b).\square$$

Examples

(1) $f(x) = x^n - 1$ with $n \in \mathbb{N}$. Then $f(x)/(x-1) \in \mathbb{Q}[x]$ is irreducible. If $\omega = e^{\frac{2\pi i}{n}}$ is a so-called primitive n'th root of unity in $\mathbb{C}$ then

$$f(x) = (x-1)(x-\omega)(x-\omega^2)\cdots(x-\omega^{n-1}).$$

So $f(x)$ splits completely in $\mathbb{Q}(\omega)$, called a cyclotomic field, and the roots ω^n are distinct and $\mathbb{Q}(\omega) \neq \mathbb{Q}(\omega^2)$ but $\mathbb{Q}(\omega) \approx \mathbb{Q}(\omega^2)$.

(2) $g(x) = x^n + 1$ with $n \in \mathbb{N}$. If $\eta = e^{\frac{\pi i}{n}}$

$$g(x) = (x-\eta)(x-\eta\omega)(x-\eta\omega^2)\cdots(x-\eta\omega^{n-1}).$$

So $g(x)$ splits completely in $\mathbb{Q}(\omega, \eta)$ and $\mathbb{Q}(\eta) \approx \mathbb{Q}(\eta\omega)$.