Fields and Galois Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

1. Splitting Fields

A Polynomial and its Splitting Field

- Consider a polynomial such as X^2+2.
- Extend the field $\mathbb{Q}$ to $\mathbb{Q}[i\sqrt{2}]$ by adjoining one of the complex roots of the polynomial.
- We obtain a "bonus", in that the other root $-i\sqrt{2}$ is also in the extended field.
- Over $\mathbb{Q}[i\sqrt{2}]$ we have that $X^2+2=(X-i\sqrt{2})(X+i\sqrt{2})$.
- We say that the polynomial **splits completely** (into linear factors) over $\mathbb{Q}[i\sqrt{2}]$.
- It is indeed clear that this must happen for a polynomial of degree 2, since the "other" factor must also be linear.

Another Polynomial and its Splitting Field

- Consider the cubic polynomial X^3-2, which is irreducible over $\mathbb{Q}$ (by Eisenstein's Criterion).
- Extend $\mathbb{Q}$ to $\mathbb{Q}[\alpha]$, where $\alpha = \sqrt[3]{2}$.
- We obtain the factorization $X^3-2=(X-\alpha)(X^2+\alpha X+\alpha^2)$,
- The quadratic factor is irreducible over $\mathbb{Q}[\alpha]$ (it is irreducible over $\mathbb{R}$, since the discriminant is $-3\alpha^2$).
- Over the complex field we have the factorization
$$X^3-2=(X-\alpha)(X-\alpha e^{2\pi i/3})(X-\alpha e^{-2\pi i/3}).$$
- Since $e^{\pm 2\pi i/3}=\frac{1}{2}(-1\pm i\sqrt{3})$, we can say that X^3-2 splits completely over $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$.
- The degree of the extension is 6.

The Splitting Field

- Consider a field K and a polynomial f in $K[X]$.
- We say that an extension L of K is a **splitting field for f over K**, or that $L:K$ is a **splitting field extension**, if
  (i) f splits completely over L;
  (ii) f does not split completely over any proper subfield E of L.

  Example: $\mathbb{Q}[i\sqrt{2}]$ is a splitting field for X^2+2 over $\mathbb{Q}$.

  $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ is a splitting field of X^3-2 over $\mathbb{Q}$.

Existence of a Splitting Field

Theorem

Let K be a field and let $f \in K[X]$ have degree n. Then there exists a splitting field L for f over K, and $[L:K] \le n!$.

- f has at least one irreducible factor g (which may be f itself).
  Form the field $E_1 = K[X]/\langle g\rangle$ and denote the element $X + \langle g\rangle$ by α.
  Then α has minimum polynomial g, and so $g(\alpha) = 0$.
  Hence g has a linear factor $Y - \alpha$ in the polynomial ring $E_1[Y]$.
  Moreover $[E_1 : K] = \partial g \le n$.
  We proceed inductively: Suppose that, for each r in $\{1, \ldots, n-1\}$, we have constructed an extension E_r of K, such that f has at least r linear factors in $E_r[X]$, and $[E_r : K] \le n(n-1)\cdots(n-r+1)$. Thus, in $E_r[X]$,
  $$f = (X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_r)f_r,$$
  and $\partial f_r = n - r$.

Existence of a Splitting Field (Cont'd)

- Now repeat the argument in the previous paragraph.

  Construct an extension E_{r+1} of E_r in which f_r has a linear factor $X-\alpha_{r+1}$ and $[E_{r+1}:E_r] \leq n-r$.

  We conclude that

  $$[E_{r+1}:K] = [E_{r+1}:E_r][E_r:K] \leq n(n-1)\cdots(n-r).$$

  Hence, by induction, there exists a field E_n, such that f splits completely over E_n, and $[E_n:K] \leq n!$.

  Let $L = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n) \subseteq E_n$, where $\alpha_1, \alpha_2, \ldots, \alpha_n$ (not necessarily all distinct) are the roots of f in E_n. Then:

  - f splits completely over L;
  - f cannot split completely over any proper subfield of L.

  So L is a splitting for f over K, and $[L:K] \leq [E_n:K] \leq n!$.

Example

- Consider $f = X^5 + X^4 - X^3 - 3X^2 - 3X + 3$ in $\mathbb{Q}[X]$.
  It has two irreducible factors $f = (X^3 - 3)(X^2 + X - 1)$.
  Let $\alpha = \sqrt[3]{3}$, and let $\gamma = \frac{-1+\sqrt{5}}{2}$, $\delta = \frac{-1-\sqrt{5}}{2}$ be the roots of $X^2 + X - 1$.
  We following the procedure in the proof of the theorem.
  - Adding the root α of f, $E_1 = \mathbb{Q}(\alpha)$.
    Then $f = (X - \alpha)(X^2 + \alpha X + \alpha^2)(X^2 + X - 1)$.
  - Adding the root $\alpha e^{2\pi i/3}$ of $X^2 + \alpha X + \alpha^2$, $E_2 = E_1(\alpha e^{2\pi i/3})$.
    Then $f = (X - \alpha)(X - \alpha e^{2\pi i/3})(X - \alpha e^{-2\pi i/3})(X^2 + X - 1)$.
  - Adding the root $\alpha e^{-2\pi i/3}$ of $X - \alpha e^{-2\pi i/3}$, $E_3 = E_2(\alpha e^{-2\pi i/3})$.
    Then $f = (X - \alpha)(X - \alpha e^{2\pi i/3})(X - \alpha e^{-2\pi i/3})(X^2 + X - 1)$.
  - Adding the root γ of $X^2 + X - 1$, $E_4 = E_3(\gamma)$.
    Then $f = (X - \alpha)(X - \alpha e^{2\pi i/3})(X - \alpha e^{-2\pi i/3})(X - \gamma)(X - \delta)$.
  - Adding the root δ of $X - \delta$, $E_5 = E_4(\delta)$.
    Then $f = (X - \alpha)(X - \alpha e^{2\pi i/3})(X - \alpha e^{-2\pi i/3})(X - \gamma)(X - \delta)$.

Example (Cont'd)

- We constructed the tower of extensions

$$\begin{aligned}\mathbb{Q} \subseteq E_1 = \mathbb{Q}(\alpha) \subseteq E_2 = E_1(\alpha e^{2\pi i/3}) \\ \subseteq E_3 = E_2(\alpha e^{-2\pi i/3}) \subseteq E_4 = E_3(\gamma) \subseteq E_5 = E_4(\delta).\end{aligned}$$

  We have

$$[E_1 : \mathbb{Q}] = 3,\ [E_2 : E_1] = 2,\ [E_3 : E_2] = 1,\ [E_4 : E_3] = 2,\ [E_5 : E_4] = 1.$$

  So $[E_5 : \mathbb{Q}] = 12$.
  The field $E_5 = \mathbb{Q}(\alpha, \alpha e^{\frac{2\pi i}{3}}, \alpha e^{\frac{-2\pi i}{3}}, \gamma, \delta)$ is a splitting field for f.
- Note that, once we know the roots of f in $\mathbb{C}$, it is easy to see that a splitting field for f over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{3}, i\sqrt{3}, \sqrt{5})$.

Uniqueness of Splitting Field

Theorem

Let K and K' be fields, and let $\varphi : K \to K'$ be an isomorphism, extending to an isomorphism $\widehat{\varphi} : K[X] \to K'[X]$. Let $f \in K[X]$, and let L, L' be (respectively) splitting fields of f over K and $\widehat{\varphi}(f)$ over K'. Then there is an isomorphism $\varphi^* : L \to L'$ extending φ.

- Suppose that $\partial f = n$ and that in $L[X]$ we have the factorization

$$f = \alpha(X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_n),$$

where α, the leading coefficient of f, lies in K, and $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$. We may suppose that, for some $m \in \{0, 1, \ldots, n\}$:
  - The roots $\alpha_1, \alpha_2, \ldots, \alpha_m$ are not in K;
  - The roots $\alpha_{m+1}, \ldots, \alpha_n \in K$.

We prove the theorem by induction on m.

Uniqueness of Splitting Field (Cont'd)

- If $m=0$, then all the roots are in K. So K is a splitting field for f. Hence, in $K'[X]$,

$$\widehat{\varphi}(f)=\varphi(\alpha)(X-\varphi(\alpha_1))(X-\varphi(\alpha_2))\cdots(X-\varphi(\alpha_n)).$$

  Thus, K' is a splitting field for $\widehat{\varphi}(f)$. So $\varphi^*=\varphi$.

  Suppose now that $m>0$. We make the inductive hypothesis that, for every field E and every polynomial g in $E[X]$ having fewer than m roots outside E in a splitting field L of g, every isomorphism of E can be extended to an isomorphism of L.

  Our assumption that $m>0$ implies that the irreducible factors of f in $K[X]$ are not all linear.

Uniqueness of Splitting Field (Conclusion)

- Let f_1 be a non-linear irreducible factor of f.

  Then $\widehat{\varphi}(f_1)$ is an irreducible factor of $\varphi(f)$ in K'.

  The roots of f_1 in the splitting field L are among α_1, α_2, ..., α_n.

  Suppose, without loss of generality, that α_1 is a root of f_1.

  Similarly, the list $\varphi(\alpha_1)$, $\varphi(\alpha_2)$, ..., $\varphi(\alpha_n)$ of roots of $\widehat{\varphi}(f)$ includes a root $\beta_1 = \varphi(\alpha_i)$ of $\widehat{\varphi}(f_1)$ (we cannot assume that $i = 1$).

  By the theorem, there is an isomorphism $\varphi' : K(\alpha_1) \to K'(\beta_1)$ extending φ.

  Since f now has fewer than m roots outside $K(\alpha_1)$, we can use the inductive hypothesis to assert the existence of an isomorphism $\varphi^* : L \to L'$ extending $\varphi' : K(\alpha_1) \to K'(\beta_1)$.

  Since φ' extends ϕ, $\varphi^* : L \to L'$ also extends $\varphi : K \to K'$.

Example

- We determine the splitting field over $\mathbb{Q}$ of the polynomial $X^4 - 2$, and find its degree over $\mathbb{Q}$.

  The polynomial $X^4 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion. Over the complex field we have the factorization

  $$X^4 - 2 = (X - \alpha)(X + \alpha)(X - i\alpha)(X + i\alpha),$$

  where $\alpha = \sqrt[4]{2}$. So the splitting field of $X^4 - 2$ is $\mathbb{Q}(\alpha, i)$.

  - The minimum polynomial of α over $\mathbb{Q}$ certainly divides $X^4 - 2$. As $X^4 - 2$ is irreducible, there are no proper divisors of $X^4 - 2$ in $\mathbb{Q}[X]$. So the minimum polynomial is $X^4 - 2$. Thus, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.
  - Also, $i \notin \mathbb{Q}(\alpha)$, since $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$. Since i is a root of $X^2 + 1$, $[\mathbb{Q}(\alpha, i) : Q(\alpha)] = 2$.

  Hence $[\mathbb{Q}(\alpha, i) : \mathbb{Q}] = 8$.
- We know that every polynomial in $\mathbb{Q}$ splits completely over $\mathbb{C}$.

  So the splitting field can always be presented as a subfield of $\mathbb{C}$.

Example (Irreducibility in $\mathbb{Z}_3$)

- In the polynomial ring $\mathbb{Z}_3[X]$ there are 9 quadratic monic polynomials. Taking $\mathbb{Z}_3$ as $\{0,1,-1\}$, we can write these down as

$$\begin{array}{lll} X^2, & X^2+1, & X^2-1, \\ X^2+X, & X^2+X+1, & X^2+X-1, \\ X^2-X, & X^2-X+1, & X^2-X-1. \end{array}$$

  We can test for irreducibility of these polynomials by determining whether they have roots in $\mathbb{Z}_3$.
  - It is clear that X^2, X^2+X and X^2-X have 0 as a root;
  - X^2-1 has the root 1.
  - X^2+X+1 has the root 1.
  - X^2-X+1 has the root -1.

  The remaining polynomials X^2+1, X^2+X-1, X^2-X-1 are irreducible over $\mathbb{Z}_3$.

Example (Splitting over $\mathbb{Z}_3$)

- The field $L = \mathbb{Z}_3[X]/\langle X^2+1\rangle$ contains an element $\alpha(= X + \langle X^2+1\rangle)$, such that $\alpha^2+1=0$.

  In the ring $L[X]$, X^2+1 splits completely into $(X-\alpha)(X+\alpha)$.

  In fact L is the splitting field for X^2+1 over $\mathbb{Z}_3$.
- Similarly:
  - $\mathbb{Z}_3[X]/\langle X^2+X-1\rangle$ is the splitting field for X^2+X-1;
  - $\mathbb{Z}_3[X]/\langle X^2-X-1\rangle$ is the splitting field for X^2-X-1.

Example (Identification of Splitting Fields)

- We came up with the splitting fields
$$\mathbb{Z}_3[X]/\langle X^2+1\rangle, \quad \mathbb{Z}_3[X]/\langle X^2+X-1\rangle, \quad \mathbb{Z}_3[X]/\langle X^2-X-1\rangle$$
of the polynomials X^2+1, X^2+X-1 and X^2-X-1 over $\mathbb{Z}_3$.
Observe that, in L (with $\alpha^2=-1$),
$$\begin{aligned} (\alpha+1)^2+(\alpha+1)-1 &= (\alpha^2-\alpha+1)+(\alpha+1)-1 \\ &= (-1-\alpha+1)+(\alpha+1)-1=0; \\ (-\alpha+1)^2+(-\alpha+1)-1 &= (-1+\alpha+1)+(-\alpha+1)-1=0. \end{aligned}$$
    - In $L[X]$, X^2+X-1 factorizes into $(X-(\alpha+1))(X-(-\alpha+1))$. So L is also a splitting field for X^2+X-1 over $\mathbb{Z}_3$.
    - In $L[X]$, $X^2-X-1=(X-(\alpha-1))(X-(-\alpha-1))$. So L is also a splitting field for X^2-X-1 over $\mathbb{Z}_3$.

  By the theorem,
$$\mathbb{Z}_3[X]/\langle X^2+1\rangle \cong \mathbb{Z}_3[X]/\langle X^2+X-1\rangle \cong \mathbb{Z}_3[X]/\langle X^2-X-1\rangle.$$

Example (Isomorphisms Between Splitting Fields)

- $\mathbb{Z}_3[X]/\langle X^2+X-1\rangle$ is generated over $\mathbb{Z}_3$ by an element $\beta(=X+\langle X^2+X-1\rangle)$, such that $\beta^2+\beta-1=0$.

  The mapping that fixes the elements of $\mathbb{Z}_3$ and sends β to $\alpha+1$ is an isomorphism from $\mathbb{Z}_3[X]/\langle X^2+X-1\rangle$ onto $\mathbb{Z}_3[X]/\langle X^2+1\rangle$.
- Similarly, $\mathbb{Z}_3[X]/\langle X^2-X-1\rangle$ is generated over $\mathbb{Z}_3[X]$ by an element γ, such that $\gamma^2-\gamma-1=0$.

  The mapping that fixes $\mathbb{Z}_3$ and sends γ to $\alpha-1$ is an isomorphism from $\mathbb{Z}_3[X]/\langle X^2-X-1\rangle$ onto $\mathbb{Z}_3[X]/\langle X^2+1\rangle$.