Modern Algebra 2 — Lecture notes
MAT 514/614, Spring 2025 — D. Ivanšić

20 Extension Fields

Definition. A field E is an *extension field of a field* F if $F \subseteq E$ and the operations of F are operations on E restricted to F.

Examples.

$\{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\}$ is an ext. field of $\mathbf{Q}$ $\qquad$ $\{a + bi \mid a, b \in \mathbf{R}\}$ is an ext. field of $\mathbf{R}$

Fundamental Theorem of Field Theory 20.1. Let F be a field and $f \in F[x]$ a nonconstant polynomial. Then there exists an extension field E of F in which f has a zero.

Proof.

Example. Let $f(x) = (x^2+1)(x^3+2x+2) \in \mathbf{Z}_3[x]$, where the factors are irreducible. Show there is an extension field of F containing a zero of f with 9 elements and there is one with 27 elements.

Definition. Let E be an extension field of F, and let $a_1, \ldots, a_n \in E$. We set

$$F(a_1, \ldots, a_n) = \bigcap_{\text{field } G \subseteq E,\ \{a_1, \ldots, a_n\} \subseteq G} G,$$

the smallest subfield of F that contains $\{a_1, \ldots, a_n\}$.

Definition. Let E be an extension field of F and let $f \in F[x]$, $\deg f \geq 1$. We say f splits in E if there are elements $a \in F$ and $a_1, \ldots, a_n$ such that

$$f(x) = a(x - a_1) \ldots (x - a_n)$$

We call E a splitting field for f over F if $E = F(a_1, \ldots, a_n)$.

Note. One can't say "E is a splitting field for f" — the underlying field needs to be specified, so "E is a splitting field for f over F —- just like one doesn't say "f is irreducible," but "f is irreducible over F."

Example. Let $p(x) = x^2 - 2$, which is irreducible over $\mathbf{Q}$. Show that p splits in $\mathbf{R}$, but a splitting field for p over $\mathbf{Q}$ is $\mathbf{Q}[\sqrt{2}]$.

Theorem 20.2. Let F be a field and $f \in F[x]$ nonconstant. Then there exists a splitting field E for f over F.

Proof.

Example. Construct the splitting field of $x^3 + 2x + 1 \in \mathbf{Z}_3[x]$ over $\mathbf{Z}_3$.

Example. Construct the splitting field of $(x^2 - 3)(x^2 + 5) \in \mathbf{Q}[x]$ over $\mathbf{Q}$.

Theorem 20.3. Let F be a field and let $p \in F[x]$ be irreducible over F. If a is a zero of p in some extension E of F, then $F(a)$ is isomorphic to $F[x]/\langle p \rangle$. Furthermore, if $\deg f = n$, then every element of $F(a)$ can be uniquely expressed as

$$c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + \cdots + c_1 a + c_0$$

for some $c_0, \ldots, c_{n-1} \in F$.

Proof.

Corollary. Let F be a field and let $p \in F[x]$ be irreducible over F. If a is a zero of p in some extension E of F and b is a zero of p in some extension E' of F, then the fields $F(a) \subseteq E$ and $F(b) \subseteq E'$ are isomorphic.

Proof.

If F and F' are fields and $\phi : F \to F'$ is a ring homomorphism, we can build a natural extension $\phi : F[x] \to F'[x]$ that is also a ring homomorphism.

Lemma. Let F be a field, let $p \in F[x]$ be irreducible over F and let a be a zero of p in some extension of F. If $\phi : F \to F'$ is a field isomorphism and b is a zero of $\phi(p)$ in some extension of F', then there is an isomorphism from $F(a)$ to $F'(b)$ that agrees with ϕ on F and sends a to b.

Proof.

Theorem 20.4. Let $\phi : F \to F'$ be a field isomorphism and let $f \in F[x]$. If E is a splitting field for f over F and E' is a splitting field for $\phi(f)$ over F', then there is an isomorphism from E to E' that agrees with ϕ on F.

Proof.

Corollary. Let F be a field and let $f \in F[x]$. Then any two splitting fields of f over F are isomorphic.

Proof.

32 Introduction to Galois Theory

Definition. Let E be an extension field of the field F. Then we may view E as a vector space over the field F. The *degree* $[E : F]$ *of the extension* E *over* F is the dimension of that E has as a vector space over F. If $[E : F]$ is finite, then we call E a *finite extension* of F, otherwise it is said to be an *infinite extension* of F.

Example. $\mathbf{C}$ is a degree-2 extension of $\mathbf{R}$.

Example. If $p \in F[x]$ is an irreducible polynomial of degree n, then $F[x]/\langle p \rangle$ is a degree-n extension of F.

Example. $\mathbf{R}$ is an infinite extension of $\mathbf{Q}$. To verify, show that for every $n \in \mathbf{N}$, $\{\sqrt[n]{2}, \sqrt[n]{2}^2, \dots, \sqrt[n]{2}^{n-1}\}$ is a linearly independent set over $\mathbf{Q}$.

Definition. Let E be an extension field of the field F. The *Galois group of* E *over* F, denoted $\mathrm{Gal}(E/F)$, is the set of all automorphisms of E that keep the elements of F fixed. For a subgroup $H \le \mathrm{Gal}(E/F)$, we define the *fixed field of* H as

$$E_H = \{x \in E \mid \phi(x) = x \text{ for all } \phi \in H\} \qquad \text{(note that } F \subseteq E_H \text{ for every } H)$$

Note. There is no actual or implied quotient in $\mathrm{Gal}(E/F)$, this is simply how the notation for this group — unfortunately — evolved.

Note. If E is an extension of $\mathbf{Q}$, any automorphism of E automatically fixes $\mathbf{Q}$, so $\mathrm{Gal}(E/\mathbf{Q}) = \mathrm{Aut}(E)$.

Proposition. Let E be an extension field of F.

1) For any polynomial $f \in F[x]$, if α is a zero of f in E, then for any $\phi \in \mathrm{Gal}(E/F)$, $\phi(\alpha)$ is also a zero of f.
2) Let $p \in F[x]$ be irreducible over F, $K = F(\alpha) \approx F[x]/\langle p \rangle$ an extension of F. If $\varphi : F \to F$ is any automorphism of F and $\beta \in K$ a zero of p, then there exists an extension $\phi : K \to K$ such that $\phi(\alpha) = \beta$ and $\phi|_F = \varphi$. If $\deg p = n$, $\phi(\sum_{i=0}^{n-1} a_i \alpha^i) = \sum_{i=0}^{n-1} \varphi(a_i)\beta^i$.
3) Let $p \in F[x]$ be irreducible over F, and $\alpha \in E$ a zero of p. If every zero of p in E is in $F(\alpha)$, then for every $\phi \in \mathrm{Gal}(E/F)$ we have $\phi(F(\alpha)) = F(\alpha)$.

Proof.

Example. Consider the extension $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{3})$. Find all elements of $\text{Gal}(\mathbf{Q}(\sqrt{3})/\mathbf{Q})$.

Example. Consider the extension $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{3}, \sqrt{5})$. Find all elements of $\text{Gal}(\mathbf{Q}(\sqrt{3}, \sqrt{5})/\mathbf{Q})$.

Example. Consider the extension $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt[3]{2}, \omega)$, where $\omega = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$ is the primitive third root of 1. Find all elements of $\mathrm{Gal}(\mathbf{Q}(\sqrt[3]{2}, \omega)/\mathbf{Q})$.

In previous examples, we observed a correspondence between the lattice of subfields of E containing F and the lattice of subgroups of $\mathrm{Gal}(E/F)$. We consider the general situation.

Definition. Let E be an extension field of the field F. Let $\mathcal{F} = \{K \mid F \subseteq K \subseteq E\}$ be the collection of subfields "between" F and E and let $\mathcal{G}$ be the collection of subgroups of $\mathrm{Gal}(E/F)$.

1) Define $i : \mathcal{F} \to \mathcal{G}$ by $i(K) = \mathrm{Gal}(E/K)$. Note that $\mathrm{Gal}(E/K) \leq \mathrm{Gal}(E/F)$.
2) Define $j : \mathcal{G} \to \mathcal{F}$ by $j(H) = E_H$, the subfield of E on which every element of H is fixed. Note that $F \subseteq E_H$ for every $H \subseteq \mathrm{Gal}(E/F)$.
3) For $K, L \in \mathcal{F}$ and $G, H \in \mathcal{G}$ it is easy to see that if $K \subseteq L$, then $i(K) \supseteq i(L)$ and if $G \subseteq H$, then $j(G) \supseteq j(H)$, so i, j are inclusion-reversing maps between $\mathcal{F}$ and $\mathcal{G}$.
4) Furthermore, $ji(K) \supseteq K$ and $ij(H) \supseteq H$.

The following theorem states that, when E is a certain type of extension of F, the maps i and j are inverses of each other.

Fundamental Theorem of Galois Theory 32.1. Let F be a field of characteristic 0 or a finite field. If E is the splitting field over F of some polynomial in $F[x]$, then the mapping $i : \mathcal{F} \to \mathcal{G}$ is a bijection. Furthermore, for any subfield K, $F \subseteq K \subseteq E$, we have:

1) $[E : K] = |\,\mathrm{Gal}(E/K)|$ and $[K : F] = \mathrm{Gal}(E/F)/\,\mathrm{Gal}(E/K)$, so the index of $\mathrm{Gal}(E/K)$ in $\mathrm{Gal}(E/F)$ is the degree of K over F.
2) If K is the splitting field of some polynomial in $F[x]$, then $\mathrm{Gal}(E/K)$ is a normal subgroup of $\mathrm{Gal}(E/F)$ and $\mathrm{Gal}(K/F) \approx \mathrm{Gal}(E/F)/\,\mathrm{Gal}(E/K)$.
3) $K = E_{\mathrm{Gal}(E/K)}$, in other words $ji = id$.
4) If $H \leq \mathrm{Gal}(E/F)$, then $H = \mathrm{Gal}(E/E_H)$, in other words $ij = id$.

Definition. Let F be a field, $f \in F[x]$. We say that f is *solvable by radicals over* F if f splits in some extension $F(a_1, \ldots, a_n)$ of F and there exist $k_1, \ldots, k_n \in \mathbf{N}$ such that $a_1^{k_1} \in F$ and $a_i^{k_i} \in F(a_1, \ldots, a_{i-1})$ for $i = 2, \ldots, n$.

Example. Every degree-2 polynomial is solvable by radicals over $\mathbf{Q}$. Show this on the example of $p(x) = x^2 - x - 1$. Note that $a_1, \ldots, a_n$ need not be zeros of f.

Solvability by radicals means that every zero of f can be written as an expression using addition, subtraction, multiplication and division of elements of F and roots of elements of F. We know the quadratic formula gives the zeros of a degree-2 polynomial as such an expression in terms of the polynomial's coefficients. Formulas of this type also exist for degree-3 and -4 polynomials. What about a general degree-n polynomial?

Definition. We say a group G is *solvable* if there exists a *normal series* of subgroups

$$\{e\} = H_0 \subseteq H_1 \subseteq H_2 \subseteq \cdots \subseteq H_k = G$$

such that H_i is normal in H_{i+1} and H_{i+1}/H_i is abelian for all $i = 1, \ldots k - 1$.

Example. Abelian groups, dihedral groups, groups of order p^n for a prime p are all solvable. A nonabelian group containing no normal subgroups other than the trivial ones is not solvable.

Example. The splitting field of $x^n - 1$ over $\mathbf{Q}$ is $\mathbf{Q}(\omega)$, where $\omega = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$. The splitting field of $x^n - a$ is $\mathbf{Q}(\omega, b)$ where b is such that $b^n = a$. Note $b \in \mathbf{R}$ if $a > 0$. The roots of $x^n - a$ are $b, \omega b, \ldots, \omega^{n-1} b$. If F is any characteristic-0 field, then the splitting field of $x^n - a$ for $a \in \mathbf{Q} \subseteq F$ contains $\mathbf{Q}(\omega, b)$.

Theorem 32.2. Let f be field of characteristic 0 and let $a \in F$. If E the splitting field of $x^n - a$ over F, then the Galois group $\mathrm{Gal}(E/F)$ is solvable.

Proof.

Theorem 32.3. A quotient group of a solvable group is solvable.

Proof.

Theorem 32.4. Let N be a normal subgroup of a group G. If N and G/N are solvable, then G is solvable.

Proof.

Theorem 32.5. Let F be a field of characteristic 0, $f \in F[x]$. Suppose f splits in $F(a_1, \ldots, a_t)$ where $a_1^{n_1} \in F$ and $a_i^{n_i} \in F(a_1, \ldots, a_{i-1})$ for $i = 2, \ldots, t$. Let E be the splitting field of f over F in $F(a_1, \ldots, a_t)$. Then $\mathrm{Gal}(E/F)$ is solvable.

Proof.

Proposition. Let $f \in \mathbf{Q}[x]$ be irreducible over $\mathbf{Q}$ and have exactly three distinct real roots. Let $E = \mathbf{Q}(a_1, \ldots, a_5)$ be the splitting field of f over $\mathbf{Q}$. Then $\mathrm{Gal}(E/\mathbf{Q})$ is not solvable.

Proof.

Example. Show that $x^5 - 16x + 2$ has exactly three real roots and is irreducible over $\mathbf{Q}$. Therefore, p is not solvable by radicals over $\mathbf{Q}$ since its $\mathrm{Gal}(E/\mathbf{Q})$ is not solvable.

Note. The example shows that, in general, zeros of a degree-5 polynomial may not be expressible using the four algebraic operations, roots and *any* rational numbers, let alone its coefficients. (The roots may still be expressible using some other functions in terms of the coefficients.)