9 Extension Fields

This is an introduction to field theory. There are two aims.

1. Application of Ring Theory. ED, PID, UFD in particular.

2. Foundation of Galois Theory, to be treated in Special Topics in Mathematics.

Review: Let F be a field, $F[x]$ the polynomial ring over F, and $f(x), p(x) \in F[x]$.

1. The only ideals of F are $\{0\}$ and F. In particular, if $\phi : F \to R$ is a ring homomorphism, then $\mathrm{Ker}\phi = \{0\}$ or F.

2. $F[x]$ is a Euclidian Domain (ED), hence a Principal Ideal Domain (PID), and thus a Unique Factorization Domain (UFD).

3. If A is a nonzero proper ideal of $F[x]$. If $f(x)$ is a nonzero polynomial in A of minimal degree, then $A = \langle f(x) \rangle$. Theorem 5.3.

4. The following are equivalent: $p(x)$ is an irreducible polynomial $\Leftrightarrow$ $\langle p(x) \rangle$ is a maximal ideal $\Leftrightarrow$ $F[x]/\langle p(x) \rangle$ is a field.

Definition 9.1 **1.** A field E is an *extension field* of a field F if F is a subring of E. In this case $1_E = 1_F$. [14]

2. Let E be an extension field of F and let $f(x) \in F[x]$. We say that $f(x)$ *splits* in E if $f(x)$ can be factored as a product of linear factors in $E[x]$. We call E a *splitting field for* $f(x)$ *over* F, if $f(x)$ splits in E but in no proper subfield of E.

3. Let E be an extension field of F and $a_1, a_2, \ldots, a_n \in E$. Then $F(a_1, a_2, \ldots, a_n)$ denotes the smallest subfield of E containing F and the set $\{a_1, a_2, \ldots, a_n\}$, i.e., the intersection of all subfields of E containing F and the set $\{a_1, a_2, \ldots, a_n\}$. (Exercise 35)

Note. If $f(x) \in F[x]$ factors as

$$(c_1x - b_1)(c_2x - b_2)\cdots(c_nx - b_n) = c(x - a_1)(x - a_2)\cdots(x - a_n),$$

with $b_1, b_2, \ldots, b_n, c_1, c_2, \ldots, c_n \in E$, $c \in F$, over some extension E of F, i.e., $a \in F$, $a_1, a_2, \ldots, a_n \in E$. Then $F(a_1, a_2, \ldots, a_n)$ is the splitting field for $f(x)$ over F in E.

Example 9.1 $\boldsymbol{Q} \subset \boldsymbol{Q}(\sqrt[4]{2}) \subset \boldsymbol{Q}(\sqrt[4]{2}, \sqrt{-1}) \subset \boldsymbol{C}$.
$f(x) = x^4 - 2 \in \boldsymbol{Q}[x]$ is irreducible over $\boldsymbol{Q}$, it has a root in $\boldsymbol{Q}(\sqrt[4]{2})$ but does not split in $\boldsymbol{Q}(\sqrt[4]{2})$. $\boldsymbol{Q}(\sqrt[4]{2}, \sqrt{-1})$ is the splitting field of $f(x)$ over $\boldsymbol{Q}$ contained in $\boldsymbol{C}$.

Lemma 9.1 (Theorem 20.1 (Kronecker, 1887)) *Let F be a field and let $f(x)$ be a nonconstant polynomial in $F[x]$. Then there is an extension field E of F in which $f(x)$ has a zero.*

---

[14] $1_E = 1_F(1_F)^{-1} = 1_F 1_F (1_F)^{-1} = 1_F$. Note that identity element in a ring R is a nonzero element e satisfying $re = r = er$ for all $r \in R$. This is the case when E is an integral domain.

Proof. Let $p(x)$ be an irreducible factor of $f(x)$. Set $E = F[x]/\langle p(x)\rangle$, and

$$\phi : F \to E \ (a \mapsto a + \langle p(x)\rangle).$$

Since $p(x)$ is irreducible, $\langle p(x)\rangle$ is a maximal ideal and E is a field. Moreover, since $p(x)$ is a factor of $f(x)$, a zero of $p(x)$ is a zero of $f(x)$. Then ϕ is an injection[15] and $\phi(F)$ can be regarded as F. Let $X = x + \langle p(x)\rangle$. Then

$$p(X) = p(x) + \langle p(x)\rangle = \langle p(x)\rangle = 0_E.$$

This proves the assertion. ■

Theorem 9.2 (Theorem 20.2) *Let F be a field and let $f(x)$ be a nonconstant element of $F[x]$. Then there exists a splitting field E for $f(x)$ over F.*

Proof. Induction on $n = \deg f(x)$. If $n = 1$, there is nothing to prove. Suppose $n \geq 2$. Then by Lemma 9.1 there is an extension E_1 of F such that $f(x)$ has a root in E_1. Now $f(x) = (x - a_1)f_1(x)$, $a_1 \in E_1$ and $f_1(x) \in E_1[x]$ with $\deg f_1(x) = n - 1$. By induction hypothesis, there is a splitting field E for $f_1(x)$ over E_1. Let $a_2, \ldots, a_n$ be roots of $f_1(x)$ in E. Then $F(a_1, a_2, \ldots, a_n)$ is the splitting field for $f(x)$ over F contained in E. ■

Example 9.2 $p(x) = x^2 + x + 1 \in \boldsymbol{Z}_2[x]$ is irreducible over $\boldsymbol{Z}_2$. $E = \boldsymbol{Z}_2[x]/\langle p(x)\rangle$ can be regarded as $\boldsymbol{Z}_2 \times \boldsymbol{Z}_2$ with usual entry-wise addition and multiplication using multiplication in $F[x]$ modulo $\langle p(x)\rangle$.

Note.

1. (*may skip*) F in Lemma 9.1 can be replaced by an integral domain, as there is a quotient field containing an integral domain.

2. (*may skip*) This is not the case if the ring is not an integral domain.

   $$f(x) = 2x + 1 \in \boldsymbol{Z}_4[x].$$

   If there exists $\beta \in R \supset \boldsymbol{Z}_4$ such that $2\beta + 1 = 0$. Then $2 = 0$, a contradiction.

Theorem 9.3 (Theorem 20.3) *Let F be a field and let $p(x) \in F[x]$ be irreducible over F. Let a be a zero of $p(x)$ in some extension F of F, then $F(a)$ is isomorphic to $F[x]/\langle p(x)\rangle$. Furthermore, if $\deg p(x) = n$, then every member of $F(a)$ can be uniquely expressed in the form*

$$c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + \cdots + c_1 a + c_0, \ \textit{where } c_0, c_1, \ldots, c_{n-1} \in F.$$

Proof. Let $\phi : F[x] \to F(a)$ $(f(x) \mapsto f(a))$. Then $\mathrm{Ker}(\phi) \supset \langle p(x)\rangle$ which is maximal. Hence equality holds. Moreover $\mathrm{Im}\phi$ is a field containing F and a. Thus surjective. The rest is clear. ■

[15] If $\phi : F \to R$ is a ring homomorphism from a field F, then $\phi = 0$ or ϕ is an injection. This is because $\mathrm{Ker}\phi$ is an ideal of a field and hence $\mathrm{Ker}\phi = \{0\}$ or F.

Corollary 9.4 *Let F be a field and let $p(x) \in F[x]$ be irreducible over F. If a is a zero of $p(x)$ in some extension E of F and b is a zero of $p(x)$ in some extension E' of F, then the fields $F(a)$ and $F(b)$ are isomorphic.*

Lemma 9.5 *Let F be a field, let $p(x) \in F[x]$ be irreducible over F, and let a be a zero of $p(x)$ in some extension of F. If ϕ is a field isomorphism from F to F' and b is a zero of $\phi(p(x))$ in some extension of F', then there is an isomorphism from $F(a)$ to $F(b)$ that agrees with ϕ on F and carries a to b.*

Proof. Let $\psi : F[x] \to F'[x]/\langle \phi(p(x)) \rangle$ $(f(x) \mapsto \phi(f(x)) + \langle \phi(p(x)) \rangle)$. Then since $\phi : F[x] \to F'[x]$ $(g(x) \mapsto \phi(g(x)))$ is an isomorphism, $\mathrm{Ker}(\psi) = \langle p(x) \rangle$ and $F[x]/\langle p(x) \rangle \approx F'[x]/\langle \phi(p(x)) \rangle$. Therefore

$$F(a) \approx F[x]/\langle p(x) \rangle \approx F'[x]/\langle \phi(p(x)) \rangle \approx F'(b)$$

as desired. ■

Theorem 9.6 (Theorem 20.4, Corollary) *Let ϕ be an isomorphism from a field F to a field F' and let $f(x) \in F[x]$. If E is a splitting field for $f(x)$ over F and E' is a splitting field for $\phi(f(x))$ over F', then there is an isomorphism from E to E' that agrees with ϕ on F.*

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

Proof. Induction on $\deg(f(x))$. It is trivial if $\deg(f(x)) = 1$. Suppose $\deg(f(x)) > 1$ and let $p(x)$ be an irreducible factor of $f(x)$, a a zero of $p(x)$ in E and b a zero of $\phi(p(x)) \in F'[x]$ in E'. Then by Lemma 9.5 there is an isomorphism α from $F(a)$ to $F'(b)$ sending a to b. Moreover $f(x) = (x-a)g(x)$ in $E[x]$ and $\phi(f(x)) = (x-b)\alpha(g(x))$. Since $\deg(g(x)) < \deg(f(x))$ and E is a splitting field for $f(x)$ over $F(a)$ and E' is a splitting field for $\phi(f(x))$ over $F'(b)$, there is an isomorphism $\psi : E \to E'$ that agrees with α on $F(a)$. Note that ψ agrees with ϕ on F. ■

Example 9.3

1. $\boldsymbol{Q}(\sqrt[4]{2}) \approx \boldsymbol{Q}[x]/\langle x^4 - 2 \rangle \approx \boldsymbol{Q}(\sqrt[4]{2}\sqrt{-1})$.
2. (*may skip*) $\boldsymbol{Q}(\sqrt[n]{2}) \approx \boldsymbol{Q}[x]/\langle x^n - 2 \rangle$.
3. Every field with 4 elements is isomorphic to $\boldsymbol{Z}_2[x]/\langle x^2 + x + 1 \rangle$.

   Let F be a field with four elements. Then its characteristic is 2 and $a^3 - 1 = (a-1)(a^2+a+1) = 0$ for every nonzero element of F. So if $a \in F \setminus \boldsymbol{Z}_2$, $a^2+a+1 = 0$. Since $x^2 + x + 1$ is irreducible over $\boldsymbol{Z}_2$, we have the assertion.

Theorem 9.7 (Theorem 20.5) *A polynomial $f(x)$ over a field F has a multiple zero in some extension E if and only if $f(x)$ and $f'(x)$ have a common factor of positive degree in $F[x]$.*

Proof. Suppose $f(x)$ has a multiple zero in some extension field E. Let $f(x) = (x-a)^2 g(x)$ in $E[x]$. Then $x - a \mid f'(x) = (x-a)(2g(x) + (x-a)g'(x)$.

If $f(x)$ and $f'(x)$ have no common divisor of positive degree in $F[x]$, then there exist $c_1(x), c_2(x) \in F[x]$ such that $c_1(x)f(x) + c_2(x)f'(x) = 1$ as $\langle f(x), f'(x) \rangle = F[x]$. This is impossible as $0 = c_1(a)f(a) + c_2(a)f'(a) = 1$ in E.

Conversely if $p(x) \mid f(x)$ and $f'(x)$, then let $p(a) = 0$ with a in some extension field E of F. Then $f(x) = (x-a)q(x)$ and $f'(x) = q(x) + (x-a)q'(x)$ and $q(a) = 0$ and $f(x)$ has a multiple root. ∎

Proposition 9.8 (Theorem 20.6) *Let $f(x)$ be an irreducible polynomial over a field F. If F has characteristic 0, then $f(x)$ has no multiple zeros. If F has characteristic $p \neq 0$, 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. If $f(x)$ has a multiple root, then $f'(x) = 0$. ∎

Definition 9.2 A field F is called *perfect* if F has characteristic 0 or if F has characteristic p and $F^p = \{a^p \mid a \in F\} = F$.

Theorem 9.9 (Theorem 20.7) *Every finite field is perfect.*

Proof. Let F be a finite field of characteristic p. The mapping $\phi : F \to F$ $(x \mapsto x^p)$. Then this is an automorphism of F. ∎

Proposition 9.10 (Theorem 20.8) *If $f(x)$ is an irreducible polynomial over a perfect field F, then $f(x)$ has no multiple roots.*

Proof. Let $f(x) = g(x^p)$ with $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$. ∎

Proposition 9.11 (Theorem 20.9) *Let $f(x)$ be an irreducible polynomial over a field F and let E be a splitting field of $f(x)$ over F. Then all the zeros of $f(x)$ in E have the same multiplicity.*

Proof. For roots a, b of $f(x)$, use isomorphism sending a to b. ∎

Corollary 9.12 *Let $f(x)$ be an irreducible polynomial over a field F and let E be a splitting field of $f(x)$. Then $f(x)$ has the form*

$$a(x-a_1)^n(x-a_2)^n \cdots (x-a_t)^n,$$

where $a_1, a_2, \ldots, a_t$ are distinct elements of E and $a \in F$.

Example 9.4 Let $F = \boldsymbol{Z}_2(t)$ be the field of quotients of the ring $\boldsymbol{Z}_2[t]$ of polynomials in the indeterminate t. Then $f(x) = x^2 - t \in F(t)[x]$ is irreducible. Note that $f(h(t)/k(t)) = 0$ yields $(h(t))^2 = t(k(t))^2$ or $h(t^2) = tk(t^2)$, a contradiction. Moreover, $f'(x) = 0$ and $f(x)$ has a multiple root. (See Exercise 39)