Chapter 20 Extension fields

Definition An extension field $\mathbb{E}$ of a given field $\mathbb{F}$ is a field such that the operations of $\mathbb{F}$ are those of $\mathbb{E}$ restricted to $\mathbb{F}$.

Theorem 20.1 Let $f(x) \in \mathbb{F}[x]$ be a nonconstant polynomial. Then there is an extension field $\mathbb{E}$ in which $f(x)$ has a zero.

Proof. May assume that $f(x)$ is irreducible; construct $\mathbb{E} = \mathbb{F}[x]/\langle f(x) \rangle$. $\square$

Example Let $f(x) = 2x + 1 \in \mathbb{Z}_4[x]$. Then $f(x)$ does not have zero in any ring R containing $\mathbb{Z}_4$ as a subring.

Proof. If $\beta \in R$ is a zero, then $0 = 2\beta + 1$ so that $0 = 2(2\beta + 1) = 4\beta + 2$, contradiction.

Splitting fields

Definition Let $\mathbb{F}$ has an extension field, and $a_1, \ldots, a_n \in \mathbb{E}$. Then $\mathbb{F}(a_1, \ldots, a_n)$ is the intersection all subfields of $\mathbb{E}$ containing $\mathbb{F} \cup \{a_1, \ldots, a_n\}$.

Definition Let $\mathbb{E}$ be an extension field of $\mathbb{F}$, and $f(x) \in \mathbb{F}[x]$ has degree $n \geq 1$. We say that $f(x)$ splits in $\mathbb{E}$ if there are $a, a_1, \ldots, a_n$ such that

$$f(x) = a(x - a_1) \cdots (x - a_n).$$

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

Theorem 20.2 Let $\mathbb{F}$ be a field and let $f(x) \in \mathbb{F}[x]$ be non-constant. Then there is a splitting field of $f(x)$.

Proof. Induct on $\deg(f(x)) = n$. If $n = 1$, then $\mathbb{E} = \mathbb{F}$. For larger n, let $g(x)$ be a irreducible factor of $f(x)$, then $\mathbb{E} = \mathbb{F}[x]/\langle g(x) \rangle$ contains a zero a_1 of $g(x)$. Then $f(x) = (x - a_1)h(x) \in \mathbb{E}[x]$. By induction assumption, there is a splitting field K of $\mathbb{E}$. One can then find a splitting field K of $f(x)$.

Example Consider $f(x) = x^4 - x^2 - 2 = (x^2 - 2)(x^2 + 1) \in \mathbb{Q}[x]$. Then the splitting field equals

$$\mathbb{Q}(\sqrt{2}, i) = \{(a + bi) + (c + di)\sqrt{2} : a, b, c, d \in \mathbb{Q}\}.$$

Theorem 20.3 Let a be a zero of the irreducible polynomial $p(x) \in \mathbb{F}[x]$. Then $\mathbb{F}(a)$ is isomorphic to $\mathbb{F}(x)/\langle p(x)\rangle$. If $p(x)$ has degree n, then $\mathbb{F}(a)$ is a vector space over $\mathbb{F}$ with a basis $\{1, a, a^2 \cdots, a^{n-1}\}$.
If b is another zero of the irreducible polynomial, then $\mathbb{F}(a)$ and $\mathbb{F}(b)$ are isomporphic.

Proof. Define $\phi : \mathbb{F}[x] \to \mathbb{F}(a)$ by $\phi(f(x)) = f(a)$. Then $Ker(\phi) = \langle p(x)\rangle$. By the isomorphism theorem, $\mathbb{F}[x]/Ker(\phi) \sim \mathbb{F}(a)$. ... □

Corollary Suppose $f(x)$ is irreducible in $\mathbb{F}[x]$ with zeros in extension fields $\mathbb{E}$ and $\mathbb{E}'$, respectively. Then $F(a)$ and $F(b)$ are isomorphic.
Proof. They are isomorphic to $\mathbb{F}[x]/\langle f(x)\rangle$. □

Theorem 20.4 Suppose $f(x) \in \mathbb{F}[x]$ with a splitting field $\mathbb{E}$. Let $\phi : \mathbb{F} \to \mathbb{F}'$ be a field isomorphism. Then $\phi(f(x))$ is irreducible in $\mathbb{F}'[x]$. If $\mathbb{E}'$ is a splitting field of $\phi(f(x))$, then there is an isomorphism from $\mathbb{E}$ to $\mathbb{E}'$ agree with ϕ on $\mathbb{F}$.

Proof. **Step 1.** Let a be a zero of an irreducible factor $p(x)$ of $f(x)$ in $\mathbb{E}$, and let b be a zero of $\phi(p(x))$ in $\mathbb{E}'$. Extend $\phi : \mathbb{F}(a) \to \mathbb{F}'(b)$ using the map sending $h(x) + \langle p(x) \rangle \in \mathbb{F}[x]/\langle p(x) \rangle$ to $\phi(h(x)) + \langle \phi(p(x)) \rangle$.

Step 2. Use induction on the degree of $f(x)$. If $f(x)$ has degree 1, then $\mathbb{F} = \mathbb{E}$ and $\mathbb{F}' = \mathbb{E}'$. The result is true.
Assume that $f(x)$ has degree $n > 1$. Now, write $f(x) = (x - a)g(x)$ and $\phi(f(x)) = (x - b)\phi(g(x))$. Use induction to finish the proof. □

Corollary Let $f(x) \in \mathbb{F}[x]$. Any two splitting fields of $f(x)$ are isomorphic.

Example The splitting field of $x^n - a \in \mathbb{Q}[x]$ equals $\mathbb{Q}(a^{1/n}, \exp(i2\pi/n))$.

Zeros of an irreducible polynomials

Definition The derivative of $f(x) = a_n x^n + \cdots + a_0$ is $f'(x) = na_n x^{n-1} + \cdots + a_1$.

Lemma Let $f(x), g(x) \in \mathbb{F}[x]$ and $a \in \mathbb{F}$. Then

$$(f(x) + g(x))' = f'(x) + g'(x), \qquad (af(x))' = af'(x),$$

$$(f(x)g(x))' = f'(x)g(x) + f(x)g'(x).$$

Theorem 20.5 A polynomial $f(x) \in \mathbb{F}[x]$ has a multiple zero in some extension field if and only if $f(x)$ and $f'(x)$ have a common factor of positive degree in $\mathbb{F}[x]$.

Proof. If $f(x) = (x-a)^2 g(x) \in \mathbb{E}[x]$, then $f'(x) = \ldots$ so that $f'(x)$ and $f'(x)$ have common factor in $\mathbb{E}$.

If $f(x)$ and $f'(x)$ have no common factor in $\mathbb{F}[x]$, i.e., they are relatively prime, then there is $g(x), h(x) \in \mathbb{F}[x]$ such that $g(x)f(x) + h(x)f'(x) = 1$ so that $(x-a)$ is a factor of $1 \in \mathbb{E}[x]$.

Conversely, if $f(x)$ and $f'(x)$ have a common factor $(x-a)$, then $f(x) = (x-a)g(x)$ and $f'(x) = g(x) + (x-a)g'(x)$ so that $g(x) = (x-a)h(x)$. Hence, $f(x) = (x-a)^2 h(x)$ in $\mathbb{E}[x]$. $\square$

Theorem 20.6 Let $f(x) \in \mathbb{F}[x]$ be irreducible. If $\mathbb{F}$ has characteristic 0, then $f(x)$ has no multiple zeros. In case $\mathbb{F}$ has characteristic p, $f(x)$ has a multiple zero if and only if $f(x) = g(x^p)$ for some $g(x) \in \mathbb{F}[x]$.

Proof. If $f(x)$ has a multiple zero, then $f(x)$ and $f'(x)$ have common factor $g(x)$ of degree at least 1 in $\mathbb{F}[x]$. Then $g(x)|f(x)$ implies that $g(x) = uf(x)$. Now, $g(x)|f'(x)$, we see that $f'(x) = 0$.

Now, $f'(x) = 0$ means $ka_k = 0$ for all $k = 1, \ldots, n$, if $f(x) = a_0 + \cdots + a_n x^n$.

If $\mathrm{Char}\mathbb{F} = 0$, then ...

If $\mathrm{Char}\mathbb{F} = p$, then ...

Structure of polynomials in their splitting fields

A field $\mathbb{F}$ is perfect if $\mathbb{F}$ has characteristic 0 or characteristic p such that $\mathbb{F}^p = \{a^p : a \in \mathbb{F}\} = \mathbb{F}$.

Theorem 20.7 Every finite field is perfect.

Proof. Suppose $\mathbb{F}$ has characteristic p. The map $x \mapsto x^p$ is a field isomorphism. □

Theorem 20.8 If $f(x) \in \mathbb{F}[x]$, where $\mathbb{F}$ is perfect, then $f(x)$ has no multiple roots.

proof. If $\mathrm{Char}\mathbb{F} = 0$, we are done.
If $\mathrm{Char}\mathbb{F} = p$, then $f(x) = \sum a_k (x^p)^k = (\sum a_k x^k)^p$, a contradiction. □

Theorem 20.9 The zeros of an irreducible polynomial $f(x) \in \mathbb{F}[x]$ have the same multiplicity. Thus, the polynomial has a factorization $a_n(x-a_1)^n(x-a_2)^n \cdots (x-a_t)^n$ with $a_1, \ldots, a_t$ in the extension field, and $a_n \in \mathbb{F}$.

Proof. Suppose $f(x) = (x-a)^m g(x) \in \mathbb{E}[x]$.
There is a field isomorphism $\phi : \mathbb{E} \to \mathbb{E}$ leaving $\mathbb{F}$ invariant and sending a to b.
Thus,

$$\phi(f(x)) = \phi((x-a)^m)\phi(g(x)) = (x-b)^m \phi(g(x)) \in \mathbb{E}[x].$$

An example

Let $\mathbb{F} = \mathbb{Z}_2(t)$ be

$$\left\{ \frac{f(t)}{g(t)} : f(t), g(t) \in \mathbb{Z}_2[t], g(t) \neq 0, f(t), g(t) \text{ have no common factor } \right\},$$

the field of quotients of $\mathbb{Z}_2[t]$. Note that $\frac{f_1(t)}{g_1(t)} = \frac{f_2(t)}{g_2(t)}$ if $f_1(t)g_2(t) = f_2(t)g_1(t)$]; $\frac{f_1(t)}{g_1(t)} + \frac{f_2(t)}{g_2(t)} = \frac{f_1(t)g_2(t)+f_2(t)g_1(t)}{g_1(t)g_2(t)} = \frac{f_3(t)}{g_3(t)}$, and $\frac{f_1(t)}{g_1(t)} \frac{f_2(t)}{g_2(t)} = \frac{f_1(t)f_2(t)}{g_1(t)g_2(t)} = \frac{f_3(t)}{g_3(t)}$.

Note also that $\mathbb{F}$ is not a perfect field.

Claim: $f(x) = x^2 - t \in \mathbb{F}[x]$.

We need to show that $f(x)$ has no zero in $\mathbb{F}$.

It suffices to show that $f(x)$ has no zero in $\mathbb{F}$, i.e., $(h(t)/g(t))^2 \neq t$.

If $h(t)^2 = tg(t)^2$, then $h(t^2) = tg(t^2)$, a contradiction. $\square$