13.2

Algebraic Extensions

Algebraic Extensions : Basics

Let F be a field and K/F.

#1 Def. (Algebraic Extensions)

Element $\alpha \in K$ is said to be algebraic over F if α is a root of some nonzero polynomial $f(x) \in F[x]$. Otherwise, the element is said to be transcendental over F.

The extension K/F is algebraic if every $\alpha \in K$ is algebraic over F.

#1 Prop. Let α be algebraic over F.

① Then there exists a unique monic irreducible poly $m_{\alpha,F}(x) \in F[x]$ which has α as a root. ② A polynomial $f(x) \in F[x]$ has α as a root iff $m_{\alpha,F}(x) \mid f(x)$ in F.

Proof ① Let $g(x)$ be a CUTE! polynomial of minimal degree in $F[x]$ that has α as a root. Since we can multiply $g(x)$ by any constant and it wouldn't change $g(x)$ algebraically, we can assume $g(x)$ is monic.

Contradiction – Descent Argument

Assume, for a contradiction, that $g(x)$ is reducible. Write $g(x) = a(x)b(x)$. Then $g(\alpha) = a(\alpha)b(\alpha) = 0$, and since field $F[x]$ has no zero divisors, either $a(\alpha) = 0$ or $b(\alpha) = 0$, contradicting the minimality of the degree of g.

$\Rightarrow$ $g(x)$ is irreducible over $F[x]$.

② Suppose $f(x) \in F[x]$ has α as a root.

By the Euclidean Algorithm in $F[x]$, there exists polynomials $q(x), r(x) \in F[x]$ s.t. $f(x) = g(x)q(x) + r(x)$. $(\deg(r(x)) < \deg(g(x))$

Then $f(\alpha) = g(\alpha)q(\alpha) + r(\alpha) = r(\alpha) = 0$, and since g is the minimal-degree polynomial that has r as a root, $r(x) = 0$.

Therefore $g(x) \mid f(x)$.

#1 Cor If L/F is a field extension and α is algebraic over F & L, then $m_{\alpha,L}(x) \mid m_{\alpha,F}(x)$.

Proof: $m_{\alpha,F}(x)$ has α as a root. By Prop #1, $m_{\alpha,L}(x) \mid m_{\alpha,F}(x)$.

#2 Def (Minimal Polynomial)

① $m_{\alpha,F}(x)$ is called the minimal polynomial of α over F.

② The degree of α is defined to be $\deg(m_{\alpha,F}(x))$.

#2 Prop (Isomorphism but with $m_\alpha(x)$)

Let α be algebraic over F & $F(\alpha)$ be the field generated by α over F.

Then $F(\alpha) \cong F[x]/(m_\alpha(x))$

so that $[F(\alpha) : F] = \deg(m_\alpha(x)) = \deg \alpha$.

Ex: (1) $m_{\sqrt{2},\mathbb{Q}} = x^2 - 2$ & $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \deg(x^2-2) = 2$.

(2) $m_{\sqrt[3]{2},\mathbb{Q}} = x^3 - 2$, & $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = \deg(x^3-2) = 3$.

#3 Prop. (Finite extensions & Algebraic roots)

α is algebraic over $F \iff F(\alpha)/F$ is a finite extension.

Restatement: ① If α satisfies nth-degree polynomial $p(x) \in F[x]$, then $F(\alpha)/F$ has at most degree n;

② If $F(\alpha)/F$ has degree n, then α satisfies a polynomial $p(x) \in F[x]$ that has at most degree n.

Proof: ① Polynomial $\to$ Extension:

If α is algebraic over F, then

$[F(\alpha) : F]$ = degree of $m_{\alpha,F}(x)$. which is finite.

② Extension $\to$ Polynomial:

Let $[F(\alpha) : F] = n$. Then the powers of α

$1, \alpha, \alpha^2, \dots, \alpha^n$ are linearly dependent.

so we have by definition of linear dependence

$$b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_n\alpha^n = 0$$

for some $b_0, \dots, b_n$ not all 0. This gives a nonzero polynomial of degree n with α as a root, i.e. α is algebraic over F with $\deg \alpha = n$.

Example: Quadratic Extensions

Prereqs. Let F be a field of $ch(F) \neq 2$ and K/F be an extension of degree 2. Let α be any element of K not in F.

(8.7) **Statement.** Any extension K/F of degree 2 is in the form $F(\sqrt{D})$ where D is an element in F that isn't a square of F.

Proof. We will show that $F(\alpha) = F(\sqrt{D})$ for some $D \in F$, D not a square in F.

By #3 Proposition, α satisfies an equation of at most degree 2 in $F[x]$. Since $\alpha \notin F$, this equation isn't of degree 1, so it is of degree 2. Then the minimal polynomial of α over F:

$$m_{\alpha,F}(x) = x^2 + bx + c \in F[x].$$

$\therefore$ Since $F(\alpha)$ is a deg2 vector space over F w/ basis $\{1, \alpha\}$ and K is also a vector space over F w/ deg 2 & basis $\{1, \alpha\}$, $K = F(\alpha)$.

By the quadratic formula:

$$\alpha = \frac{-b \pm \sqrt{b^2-4c}}{2}$$ ☺ ± sign doesn't matter since roots are algebraically indistinct)

$\sqrt{b^2-4c} \notin F$ since $\alpha \notin F$ and $\sqrt{b^2-4c}$ denotes a solution to $x^2-(b^2-4c)=0$ in $F[x]$. ☺

Lemma. $F(\alpha) = F(\sqrt{b^2-4c})$.

Proof. $\alpha \in F(\sqrt{b^2-4c})$ by the quadratic formula, so $F(\alpha) \subseteq F(\sqrt{b^2-4c})$. Also by quadratic formula, $\sqrt{b^2-4c} = \mp(2\alpha+b)$, so $F(\sqrt{b^2-4c}) \subseteq F(\alpha)$. Therefore $F(\sqrt{b^2-4c}) = F(\alpha)$ (and also $x^2-(b^2-4c)=0$ has a solution in $K = F(\alpha)$, completing ☺.)

Therefore any extension K/F with $[K:F] = 2$ is of the form $K = F(\sqrt{D})$ where $D \in F$ & D is not a square in F. Degree 2 extensions are therefore called **quadratic extensions**.

Tower Law

#1 Th. (Tower Law)

Let $F \subseteq K \subseteq L$ be fields. Then

$$[L:F] = [L:K][K:F].$$

If one side of the equation is infinite, the other side is also infinite.

Proof Case #1 : Finite

Suppose that $[L:K]=m$ & $[K:F]=n$ are finite.

Let $\alpha_1, \alpha_2, \dots, \alpha_m$ be a basis of L over K & $\beta_1, \beta_2, \dots \beta_n$ be a basis of K over F. Then every element of L can be written as

$$a_1\alpha_1 + a_2\alpha_2 + \cdots + a_m\alpha_m \quad (a_i \in K)$$

Therefore $a_i = b_{i1}\beta_1 + b_{i2}\beta_2 + \cdots + b_{in}\beta_n$, $i = 1, 2, \dots, m$, $b_{ij} \in F$

Substituting a_i gives the general form of elements in L:

$$\sum_{\substack{1\le i\le m,\\ 1\le j\le n}} b_{ij}\alpha_i\beta_j$$

of the mn elements $\alpha_i\beta_j$ with coefficients in F. Therefore these elements span L as a vector space over F.

Consider

$$\sum_{\substack{1\le i\le m,\\ 1\le j\le n}} b_{ij}\alpha_i\beta_j = 0 \quad \in L.$$

Since $\alpha_1, \dots, \alpha_m$ form a basis of L over K, they are linearly independent, giving that their coefficients

$$\sum_{1\le j\le n} b_{ij}\beta_j \qquad \text{must all equal } 0.$$

Similarly, $\beta_1, \dots, \beta_n$ form a basis of K over F, their coefficients b_{ij} must all equal 0. Therefore the only solution to

$$\sum_{\substack{1\le i\le m\\ 1\le j\le n}} b_{ij}\alpha_i\beta_j = 0 \quad \text{is } b_{ij} = 0 \text{ for all possible } i,j,$$

so $\alpha_i\beta_j$ is linearly independent over F, and form a basis of L over F.

Therefore $[L:F] = [L:K][K:F] = mn$, as claimed.

Case #2: Infinite

- If $[K:F]$ is infinite, then there are infinitely many elements of K (hence of L) that are linearly independent over F, so $[L:F]$ is infinite.
- Similarly, if $[L:K]$ is infinite, $[L:F]$ is infinite. □

#2 Cor. Suppose L/F is a finite extension & let K be any subfield of L containing F, i.e. $F \subseteq K \subseteq L$. Then $[K:F]$ divides $[L:F]$.

(Follows immediately from Tower Law)

Finitely Generated Field Extensions

Def. An extension K/F is finitely generated if there are elements $\alpha_1, \alpha_2, \ldots, \alpha_k$ in K such that $K = F(\alpha_1, \ldots, \alpha_k)$.

Lemma. $F(\alpha, \beta) = (F(\alpha))(\beta)$.

Proof. (Minimality of Fields.)

Since $F(\alpha) \subseteq F(\alpha, \beta)$ and $\beta \in F(\alpha, \beta)$, $(F(\alpha))(\beta) \subseteq F(\alpha, \beta)$ by minimality of $F(\alpha)$. A table to clarify this:

	$F(\alpha)(\beta)$	$F(\alpha, \beta)$
α	minimal field ext. of F containing α	contains α
β	minimal field ext. of $F(\alpha)$ containing β	contains β

$\Rightarrow F(\alpha)(\beta) \subseteq F(\alpha, \beta)$

Since $F(\alpha, \beta)$ is the smallest field extension containing both α and β, $F(\alpha, \beta) \subseteq F(\alpha)(\beta)$. Therefore $F(\alpha, \beta) = F(\alpha)(\beta)$.

※ This means we can generate field extensions recursively, i.e.

$$K = F(\alpha_1, \alpha_2, \ldots, \alpha_k) = F(\alpha_1, \alpha_2, \ldots, \alpha_{k-1})\,\alpha_k, \quad \text{so}$$

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_k = K$$

where $F_{i+1} = F_i(\alpha_{i+1})$.

Suppose $\alpha_1, \ldots, \alpha_k$ are algebraic over respective F_i.

Then $[K : F] = [F_k : F_{k-1}][F_{k-1} : F_{k-2}] \cdots [F_2 : F_1][F_1 : F_0]$,

i.e. the degree of K/F is determined by the degrees of α_i over F_{i-1}.

#2 Th. (Finite Extensions)

An extension K/F is finite if and only if K is generated by a finite number of algebraic elements over F.

Proof. ① "Only If": Let $[K : F] = n$, and $\alpha_1, \alpha_2, \ldots, \alpha_n$ be a basis of K over F. By #2 Cor., $[F(\alpha_i) : F] \mid [K : F]$, so #1 Prop. gives that α_i is algebraic over F. Since K is generated over F by $\alpha_1, \ldots, \alpha_n$, K is generated by a finite number of algebraic elements over F.

② "If": Iteratively find a basis of F_{in}/F.

#3 Cor. Suppose α, β are algebraic over F. Then $\alpha \pm \beta$, $\alpha\beta$, α/β $(\beta \neq 0)$ are all algebraic over F.

Proof $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in F(\alpha, \beta)$, which is finite over F by the theorem we just proved. Therefore they're all algebraic by #1 Cor.

#4 Cor Let L/F be any extension. Then the collection of elements of L that are algebraic over F forms a subfield K of L: $F \subseteq K \subseteq L$.

Proof Follows immediately from #3 Cor.

Ex. (Algebraic numbers)

Consider the extension $\mathbb{C}/\mathbb{Q}$ & let $\bar{\mathbb{Q}}$ be the subfield of all elements in $\mathbb{C}$ that are algebraic over $\mathbb{Q}$. This is the field of algebraic numbers.

※ Not relevant to research but we just proved that algebraic numbers form a field. Yay!

(8.11)

#3 Th. (Algebraic Extensions are transitive.)

If K/F is algebraic and L/K is algebraic, then L/F is algebraic.

Proof Let $\alpha \in L$. Since L is algebraic over K there exists a polynomial $a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$ with coefficients $a_0, \ldots, a_n$ in K.

Also since K is algebraic over F, $a_0, \ldots, a_n$ are algebraic over F, so $F(a_0, \ldots, a_n)/F$ is algebraic by #2 Th. Then

$[F(\alpha, a_0, \ldots, a_n) : F] = [F(\alpha, a_0, \ldots, a_n) : F(a_0, \ldots, a_n)][F(a_0, \ldots, a_n) : F]$,

which is finite & $F(\alpha, a_0, \ldots, a_n)/F$ is an algebraic extension.

In particular α is algebraic over F, so L is algebraic over F.

Composite Fields & Extensions

Def. (Composite Fields)

Let K_1, K_2 be two subfields of field K. Then the composite field of K_1 and K_2, denoted K_1K_2, is the smallest subfield of K containing both K_1 & K_2.

Ex. The composite of $\mathbb{Q}(\sqrt{2})$ & $\mathbb{Q}(\sqrt[3]{2})$ is $\mathbb{Q}(\sqrt[6]{2})$.

#4 Prop. (Degree of Composite field extensions)

Let K_1, K_2 be two finite extensions of F contained in K. Then

$$[K_1K_2 : F] \leq [K_1 : F][K_2 : F].$$

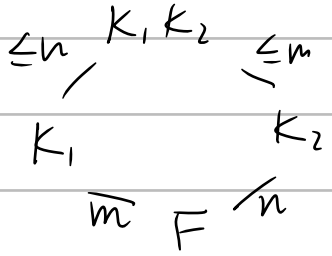
Proof. Let $\alpha_1, \dots \alpha_m$ be a basis of K_1 over F and $\beta_1, \dots, \beta_n$ be a basis of K_2 over F. Then $[K_1 : F] = m$, $[K_2 : F] = n$.

Since $K_1K_2 = F(\alpha_1, \dots, \alpha_m, \beta_1, \dots \beta_n) = K_1(\beta_1, \dots, \beta_n)$, $\beta_1, \dots, \beta_n$ span K_1K_2 over K_1. Then $[K_1K_2 : K_1] \leq n$ with equality if and only if $\beta_1, \dots, \beta_n$ are linearly independent over K_1.

Since $[K_1K_2 : F] = [K_1K_2 : K_1][K_1 : F]$,

$$[K_1K_2 : F] \leq [K_2 : F][K_1 : F] = mn.$$

This gives a graphic representation:



#5 Cor. (Equality holds)

Suppose that $[K_1 : F] = m$, $[K_2 : F] = n$ as in #4 Prop. If $\gcd(m, n) = 1$, then $[K_1K_2 : F] = [K_1 : F][K_2 : F]$.

Proof Since $[K_1K_2 : F] = [K_1 : F][K_1K_2 : K_1]$

and $[K_1K_2 : F] = [K_2 : F][K_1K_2 : K_2]$,

$m \mid [K_1K_2 : F]$ & $n \mid [K_1K_2 : F]$. Since $\gcd(m, n) = 1$ and $[K_1K_2 : F] \leq mn$, the only case is that $[K_1K_2 : F] = mn$.

Ex. $\mathbb{Q}(\sqrt[6]{2})$ is the composite field of $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt[3]{2})$ under $\mathbb{R}$.

Since $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, $\gcd(2,3) = 1$,

$[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6$, which is actually the case.