Fields and Galois Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

Subsection 1

The Degree of an Extension

Field Extensions

- If K, L are fields and $\varphi : K \to L$ is a monomorphism, we say that L is an **extension** of K.
- We write "$L : K$ is a (field) extension".
- This is not essentially different from saying that K is a subfield of L, since we may always identify K with its image $\varphi(K)$.
- Then L can be regarded as a vector space over K, since the vector space axioms are all consequences of the field axioms for L:
  - (V1) $(x+y)+z = x+(y+z)$, $x, y, z \in L$;
  - (V2) $x+y = y+x$, $x, y \in L$;
  - (V3) There exists 0 in L, such that $x+0 = x$, $x \in L$;
  - (V4) For all x in L, there exists $-x$ in L, such that $x+(-x) = 0$;
  - (V5) $a(x+y) = ax+ay$, $a \in K, x, y \in L$;
  - (V6) $(a+b)x = ax+bx$, $a, b \in K, x \in L$;
  - (V7) $(ab)x = a(bx)$, $a, b \in K, x \in L$;
  - (V8) $1x = x$, $x \in L$.

Dimension of Field Extensions

- Let $L : K$ be a field extension.
- Since L can be regarded as a vector space over K, there exists a **basis** of L over K.
- Different bases have the same cardinality, and there is a well-defined **dimension** of L, equal to the cardinality of an arbitrarily chosen basis.
- The term used in field theory for this dimension is the **degree of L over K**, or the **degree of the extension $L : K$**, denoted by $[L : K]$.
- We say that L is a **finite extension** of K if $[L : K]$ is finite.
- Otherwise L is an **infinite extension**.

Examples

- The field $\mathbb{R}$ of real numbers is an infinite extension of $\mathbb{Q}$.

  Any finite extension of $\mathbb{Q}$ is countable, and $\mathbb{R}$ is not.
- The field $\mathbb{C}$ of complex numbers is a finite extension of $\mathbb{R}$, with basis $\{1, i\}$.

  Every complex number has a unique expression as $a1 + bi$, with $a, b \in \mathbb{R}$.
- Of course, bases are not unique.
- For $\mathbb{C} : \mathbb{R}$, we can write $a + bi$ as

$$\frac{1}{2}(a+b)(1+i) + \frac{1}{2}(a-b)(1-i).$$

  So $\{1+i, 1-i\}$ is also a basis.

  But every basis has exactly two elements, and $[\mathbb{C} : \mathbb{R}] = 2$.

Extensions of Degree One

Theorem

Let $L : K$ be a field extension. Then $L = K$ if and only if $[L : K] = 1$.

- Suppose first that $L = K$. Then $\{1\}$ is a basis for L over K, since every element x of L is expressible as $x1$, with x in K. Thus, $[L : K] = 1$.

  Conversely, suppose that $[L : K] = 1$.

  Let $\{x\}$, where $x \neq 0$, be a basis of L over K.

  In particular, there exists a in K such that $1 = ax$. So $x = \frac{1}{a} \in K$.

  Now, let y in L. Then, there exists b in K, such that $y = bx = \frac{b}{a}$.

  Thus, $y \in K$. This proves that $L = K$.

Chain of Extensions

- Suppose we have field extensions $L:K$ and $M:L$.
  That is, there are monomorphisms $\alpha: K \to L$, $\beta: L \to M$.
  Then $\beta \circ \alpha: K \to M$ is a monomorphism, and so $M:K$ is an extension.

Theorem

Let $L:K$ and $M:L$ be field extensions. Then $[M:L][L:K]=[M:K]$.

- Let $\{a_1, a_2, \ldots, a_r\}$ be a linearly independent subset of M over L.
  Let $\{b_1, b_2, \ldots, b_s\}$ be a linearly independent subset of L over K.
  We show that $\{a_i b_j : i=1,2,\ldots,r, j=1,2,\ldots,s\}$ is a linearly independent subset of M over K.
  Suppose that $\sum_{i=1}^r \sum_{j=1}^s \lambda_{ij} a_i b_j = 0$, with $\lambda_{ij} \in K$, for all i and j.
  Rewrite as $\sum_{i=1}^r (\sum_{j=1}^s \lambda_{ij} b_j) a_i = 0$. Since the a_i are linearly independent over L, $\sum_{j=1}^s \lambda_{ij} b_j = 0$, $i=1,2,\ldots,r$. Since the b_j are linearly independent over K, $\lambda_{ij}=0$, for all i and j.

Chain of Extensions (Cont'd)

- Suppose $[M:L]$ or $[L:K]$ is infinite. Then either r or s can be made arbitrarily large. So the set $\{a_ib_j : i=1,\ldots,r, j=1,\ldots,s\}$ can be made arbitrarily large. Hence, $[M:K]$ is infinite.
  Suppose, next, that $[M:L]=r<\infty$, $[L:K]=s<\infty$. Let $\{a_1,a_2,\ldots,a_r\}$ be a basis of M over L, and $\{b_1,b_2,\ldots,b_s\}$ a basis of L over K.
  For each z in M, there exist $\lambda_1,\lambda_2,\ldots,\lambda_r$ in L, such that $z=\sum_{i=1}^r \lambda_i a_i$.
  For each λ_i there exist $\mu_{i1},\mu_{i2},\ldots,\mu_{is}$ in K such that $\lambda_i=\sum_{j=1}^s \mu_{ij}b_j$.
  Hence $z=\sum_{i=1}^r\sum_{j=1}^s \mu_{ij}(a_ib_j)$.
  We showed that the set $\{a_ib_j : i=1,\ldots,r, j=1,\ldots,s\}$ is an independent spanning set (a basis) for M over K. So $[M:K]=rs=[M:L][L:K]$.

Corollary

Let $K_1,K_2,\ldots,K_n$ be fields. Suppose that $K_{i+1}:K_i$ is an extension, for $1\le i\le n-1$. Then

$$[K_n:K_1]=[K_n:K_{n-1}][K_{n-1}:K_{n-2}]\cdots[K_2:K_1].$$

Subsection 2

Extensions and Polynomials

The Field $\mathbb{Q}[\sqrt{2}]$

- The equation $X^2 = 2$ cannot be solved within the field of rationals.
- It has the solutions $\pm\sqrt{2}$ in the field $\mathbb{R}$ of real numbers.
- In fact, its solutions lie within a subfield of $\mathbb{R}$, namely, the extension

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \text{ of } \mathbb{Q}.$$

- It is easy to verify the subfield conditions:
  - If $a + b\sqrt{2}, c + d\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, then

$$(a + b\sqrt{2}) - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2} \in \mathbb{Q}[\sqrt{2}];$$

  - if $c + d\sqrt{2} \neq 0$,

$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{(a + b\sqrt{2})(c - d\sqrt{2})}{(c + d\sqrt{2})(c - d\sqrt{2})} = \frac{ac - 2bd}{c^2 - 2d^2} + \frac{bc - ad}{c^2 - 2d^2}\sqrt{2}.$$

  Since $\sqrt{2}$ is irrational, $c^2 - 2d^2 = 0$ if and only if $c = d = 0$.

Subfield Generated by a Set

- Let K be a subfield of a field L.
- Let S be a subset of L.
- Let $K(S)$ be the intersection of all subfields of L containing $K \cup S$.
  There is at least one such subfield, namely L itself.
- It is clear that $K(S)$ is the smallest subfield containing $K \cup S$.
- $K(S)$ is called the **subfield of L generated over K by S**.
- If $S = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is finite, we write $K(S)$ as $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Characterization of Subfield Generated by a Set

Theorem

The subfield $K(S)$ of the field L coincides with the set E of all elements of L that can be expressed as quotients of finite linear combinations (with coefficients in K) of finite products of elements of S.

- Let P be the set of all finite linear combinations of finite products of elements of S. If $p, q \in P$, then $p \pm q, pq \in P$. Let $x = \frac{p}{q}$ and $y = \frac{r}{s}$ be typical elements of E, with p, q, r, s in P and $q, s \neq 0$.
  - $x - y = \frac{ps - qr}{qs} \in E$;
  - If $y \neq 0$, $\frac{x}{y} = \frac{ps}{qr} \in E$.

  Thus, E is a subfield of L containing K and S. So $K(S) \subseteq E$.
  Any subfield containing K and S must also contain:
  - All finite products of elements in S;
  - All linear combinations of such products;
  - All quotients of such linear combinations.

  In short, it must contain E. Hence, in particular, $K(S) \supseteq E$.

Simple Extensions

- If S has just one element $\alpha \notin K$, by the theorem, $K(\alpha)$ is the set of all quotients of polynomials in α with coefficients in K.
- We say that $K(\alpha)$ is a **simple extension** of K.
- The link with polynomials is important:

Theorem

Let L be a field, let K be a subfield and let $\alpha \in L$. Then one of the following two alternatives holds:

(i) $K(\alpha)$ is isomorphic to $K(X)$, the field of all rational forms with coefficients in K.

(ii) There exists a unique monic irreducible polynomial m in $K[X]$ with the property that, for all f in $K[X]$,

  (a) $f(\alpha) = 0$ if and only if $m \mid f$;
  (b) The field $K(\alpha)$ coincides with $K[\alpha]$, the ring of all polynomials in α with coefficients in K;
  (c) $[K[\alpha] : K] = \partial m$.

Proof of the Simple Extension Theorem Case (i)

- Suppose first that there is no non-zero polynomial f in $K[X]$ such that $f(\alpha)=0$. Then $\alpha \notin K$, since $f = X-\alpha$ would contradict the hypothesis.

  Note that $g(\alpha)=0$ only if g is the zero polynomial.

  Hence, there is a mapping $\varphi : K(X) \to K(\alpha)$ given by $\varphi\left(\frac{f}{g}\right) = \frac{f(\alpha)}{g(\alpha)}$.
  - It is routine to verify that φ is a homomorphism.
  - It clearly maps onto $K(\alpha)$.
  - It is both well defined and one-to-one.

    Suppose that f,g,p,q are polynomials, with $g,q \neq 0$. Then

$$\begin{aligned}\varphi\left(\frac{f}{g}\right)=\varphi\left(\frac{p}{q}\right) \quad &\text{iff} \quad f(\alpha)q(\alpha)-p(\alpha)g(\alpha)=0 \text{ in } L\\ &\text{iff} \quad fq-pg=0 \text{ in } K[X]\\ &\text{iff} \quad \frac{f}{g}=\frac{p}{q} \text{ in } K(X).\end{aligned}$$

Proof of the Simple Extension Theorem Case (ii)

- Suppose there exists a non-zero polynomial g such that $g(\alpha) = 0$.

  Assume that g is a polynomial with least degree having this property. If a is the leading coefficient of g, then $\frac{g}{a}$ is monic. Denote $\frac{g}{a}$ by m.
  - Certainly $m(\alpha) = 0$.
  - Clearly, if $m \mid f$, then $f(\alpha) = 0$.
    Conversely, suppose that $f(\alpha) = 0$. Then, $f = qm + r$, where $\partial r < \partial m$. Now $0 = f(\alpha) = q(\alpha)m(\alpha) + r(\alpha) = 0 + r(\alpha) = r(\alpha)$. Since $\partial r < \partial m$, r is the zero polynomial. Hence $f = qm$. So $m \mid f$.

  m is unique. Suppose that m' is another polynomial with the same properties. Then $m(\alpha) = m'(\alpha) = 0$. So $m \mid m'$ and $m' \mid m$. Since both polynomials are monic, $m' = m$.

  m is irreducible. Suppose that there exist polynomials p and q, such that $pq = m$, with $\partial p, \partial q < \partial m$. Then $p(\alpha)q(\alpha) = m(\alpha) = 0$. So either $p(\alpha) = 0$ or $q(\alpha) = 0$. This is impossible, since both p and q are of smaller degree than m.

Proof of the Simple Extension Theorem Case (ii) (Cont'd)

- $K(\alpha) = K[\alpha]$. Consider a typical element $\frac{f(\alpha)}{g(\alpha)}$ in $K(\alpha)$, $g(\alpha) \neq 0$.

  Then m does not divide g. Since m has no divisors other than itself and 1, the greatest common divisor of g and m is 1.

  Hence, there exist polynomials a, b, such that $ag + bm = 1$. Substituting α for X, $a(\alpha)g(\alpha) = 1$. Thus, $\frac{f(\alpha)}{g(\alpha)} = f(\alpha)a(\alpha) \in K[\alpha]$.

  We close by showing that $[K[\alpha] : K] = \partial m$.

  Let $\partial m = n$ and $p(\alpha) \in K[\alpha] = K(\alpha)$, where p is a polynomial.

  Then $p = qm + r$, where $\partial r < \partial m = n$. Therefore, $p(\alpha) = r(\alpha)$.

  So there exist $c_0, c_1, \ldots, c_{n-1}$ (the coefficients of r, some of which may, of course, be zero) in K, such that

  $$p(\alpha) = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}.$$

  Hence $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a spanning set for $K[\alpha]$.

Proof of the Simple Extension Theorem Case (ii) (Cont'd)

- Moreover, the set $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is linearly independent over K.

  Let $a_0, a_1, \ldots, a_{n-1}$ in K be such that

  $$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0.$$

  Then $a_0 = a_1 = \cdots = a_{n-1} = 0$. Otherwise there would be a non-zero polynomial $p = a_0 + a_1X + \cdots + a_{n-1}X^{n-1}$ of degree $\leq n-1$, such that $p(\alpha) = 0$.

  Thus $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis of $K(\alpha)$ over K. So $[K(\alpha) : K] = n$.
- The polynomial m is called the **minimum polynomial** of the element α.

A Useful Consequence

Corollary

Let L be a field, let K be a subfield and let $\alpha \in L$. If $[K[\alpha] : K] = n$ and g is a monic polynomial in $K[X]$ of degree n, such that $g(\alpha) = 0$, then g is the minimum polynomial of α.

- Let m be the minimum polynomial of α.

  Since $g(\alpha) = 0$, $m \mid g$.

  Since g is monic of degree n, $m = g$.

  Hence, g must be the minimum polynomial of α.

Example

- Let α be in $\mathbb{C}$ with minimum polynomial X^2+X+1 over $\mathbb{Q}$.
  - We show that $\alpha^2-1\neq 0$;
  - We express the element $\frac{\alpha^2+1}{\alpha^2-1}$ of $\mathbb{Q}(\alpha)$ in the form $a+b\alpha$, $a,b\in\mathbb{Q}$.

We have $\alpha^2+\alpha+1=0$. So $\alpha^2-1=-\alpha-2\neq 0$.

Now we get

$$\frac{\alpha^2+1}{\alpha^2-1}=\frac{-\alpha}{-\alpha-2}=\frac{\alpha}{\alpha+2}=1-\frac{2}{\alpha+2}.$$

Dividing X^2+X+1 by $X+2$ gives

$$X^2+X+1=(X+2)(X-1)+3.$$

So $(\alpha+2)(\alpha-1)=-3$. Hence $\frac{1}{\alpha+2}=-\frac{1}{3}(\alpha-1)$. We finally get

$$\frac{\alpha^2+1}{\alpha^2-1}=1+\frac{2}{3}(\alpha-1)=\frac{1}{3}+\frac{2}{3}\alpha.$$

Example

- If K is the field $\mathbb{Q}$ and L the field $\mathbb{C}$, the minimum polynomial of $i\sqrt{3}$ is X^2+3.

  Then
  $$\mathbb{Q}[i\sqrt{3}] = \{a+bi\sqrt{3} : a,b \in \mathbb{Q}\}.$$
  The multiplicative inverse of a non-zero element $a+bi\sqrt{3}$ is
  $$\begin{aligned} a'+b'i\sqrt{3} &= \frac{1}{a+bi\sqrt{3}} = \frac{a-bi\sqrt{3}}{(a+bi\sqrt{3})(a-bi\sqrt{3})} \\ &= \frac{a-bi\sqrt{3}}{a^2+3b^2} = \frac{a}{a^2+3b^2} - \frac{b}{a^2+3b^2} i\sqrt{3}. \end{aligned}$$

Example: The Subfield $\mathbb{Q}(\sqrt{2},\sqrt{3})$

- It might seem that the subfield $\mathbb{Q}(\sqrt{2},\sqrt{3})$ is not a simple extension, but in fact it coincides with the visibly simple extension $\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

  It is clear that $\sqrt{2}+\sqrt{3}\in\mathbb{Q}(\sqrt{2},\sqrt{3})$. So $\mathbb{Q}(\sqrt{2}+\sqrt{3})\subseteq\mathbb{Q}(\sqrt{2},\sqrt{3})$.

  Note $(\sqrt{3}+\sqrt{2})(\sqrt{3}-\sqrt{2})=1$. So $\sqrt{3}-\sqrt{2}=\frac{1}{\sqrt{3}+\sqrt{2}}\in\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

  Now we have

$$\sqrt{2}=\tfrac{1}{2}(\sqrt{2}+\sqrt{3})+\tfrac{1}{2}(\sqrt{2}-\sqrt{3})\in\mathbb{Q}(\sqrt{2}+\sqrt{3});$$
$$\sqrt{3}=\tfrac{1}{2}(\sqrt{2}+\sqrt{3})-\tfrac{1}{2}(\sqrt{2}-\sqrt{3})\in\mathbb{Q}(\sqrt{2}+\sqrt{3}).$$

  Hence $\mathbb{Q}(\sqrt{2},\sqrt{3})\subseteq\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Example: The Subfield $\mathbb{Q}(\sqrt{2},\sqrt{3})$ (Cont'd)

- We can write $\mathbb{Q}(\sqrt{2},\sqrt{3})$ as $(\mathbb{Q}[\sqrt{2}])[\sqrt{3}]$.
  The set $\{1,\sqrt{2}\}$ is clearly a basis for $\mathbb{Q}[\sqrt{2}]$ over $\mathbb{Q}$.
  Since $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$, we must have $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : Q[\sqrt{2}]] \geq 2$.
  On the other hand, observe $(\sqrt{3})^2 - 3 = 0$. So $X^2 - 3$ is the minimum polynomial of $\sqrt{3}$ over $\mathbb{Q}[\sqrt{2}]$. So $\{1,\sqrt{3}\}$ is a basis.
  Hence $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ is a basis for $\mathbb{Q}(\sqrt{2},\sqrt{3})$ over $\mathbb{Q}$.
  The minimum polynomial of $\sqrt{2}+\sqrt{3}$ is of degree 4.
  We have
  $$(\sqrt{2}+\sqrt{3})^2 = 2+2\sqrt{6}+3 = 5+2\sqrt{6};$$
  $$(\sqrt{2}+\sqrt{3})^4 = (5+2\sqrt{6})^2 = 25+20\sqrt{6}+24 = 49+20\sqrt{6}.$$
  Hence, we obtain
  $$(\sqrt{2}+\sqrt{3})^4 - 10(\sqrt{2}+\sqrt{3})^2 + 1 = 49+20\sqrt{6}-50-20\sqrt{6}+1 = 0.$$
  So the minimum polynomial is $X^4 - 10X^2 + 1$.

Algebraic and Transcendental Extensions

- If α has a minimum polynomial over K,
  - α is called **algebraic over** K;
  - $K[\alpha](=K(\alpha))$ is called a **simple algebraic extension of** K.
- A complex number that is algebraic over $\mathbb{Q}$ is called an **algebraic number**.
- If $K(\alpha)$ is isomorphic to the field $K(X)$ of rational functions,
  - α is called **transcendental over** K;
  - $K(\alpha)$ is called a **simple transcendental extension of** K.
- A complex number that is transcendental over $\mathbb{Q}$ is called a **transcendental number**.

  Example: The preceding examples feature simple algebraic extensions.

  The elements $i\sqrt{3}, \sqrt{2}, \sqrt{3}, \sqrt{2}+\sqrt{3}$ are algebraic numbers.

  On the other hand, let $L = K(X)$ be the field of rational forms over X.

  By the definitions, the element X is transcendental over K.

Algebraic, Transcendental Extensions and Degrees

Theorem

Let $K(\alpha)$ be a simple transcendental extension of a field K. Then the degree of $K(\alpha)$ over K is infinite.

- The elements $1, \alpha, \alpha^2, \ldots$ are linearly independent over K.
- An extension L of K is said to be an **algebraic extension** if every element of L is algebraic over K.
- Otherwise, L is called a **transcendental extension**.

Theorem

Every finite extension is algebraic.

- Let L be a finite extension of K. Suppose, for a contradiction, that L contains an element α that is transcendental over K. Then the elements $1, \alpha, \alpha^2, \ldots$ are linearly independent over K. So $[L : K]$ cannot be finite.

Algebraicity and Chains of Extensions

Theorem

Let $L:K$ and $M:L$ be field extensions, and let $\alpha \in M$. If α is algebraic over K, then it is also algebraic over L.

- Since α is algebraic over K, there exists a non-zero polynomial f in $K[X]$, such that $f(\alpha)=0$. Since f is also in $L[X]$, we deduce that α is algebraic over L.
- The minimum polynomial of α over L may of course be of smaller degree than the minimum polynomial over K.

  Example: We saw $[\mathbb{Q}[\sqrt{2}+\sqrt{3}]:\mathbb{Q}]=4$ and $[\mathbb{Q}[\sqrt{2}+\sqrt{3}]:\mathbb{Q}[\sqrt{2}]]=2$. We can verify that:
  - $(\sqrt{2}+\sqrt{3})^4-10(\sqrt{2}+\sqrt{3})^2+1=0$;
  - $(\sqrt{2}+\sqrt{3})^2-2\sqrt{2}(\sqrt{2}+\sqrt{3})-1=0$.

  So the minimum polynomial of $\sqrt{2}+\sqrt{3}$
  - over $\mathbb{Q}$ is X^4-10X^2+1;
  - over $\mathbb{Q}[\sqrt{2}]$ is $X^2-2\sqrt{2}X-1$.

Subfield of Algebraic Elements

Theorem

Let L be an extension of a field K, and let $\mathscr{A}(L)$ be the set of all elements in L that are algebraic over K. Then $\mathscr{A}(L)$ is a subfield of L.

- Suppose that $\alpha, \beta \in \mathscr{A}(L)$. Then $\alpha - \beta \in K(\alpha, \beta) = (K[\alpha])[\beta]$.

  By the theorem, β is algebraic over $K[\alpha]$.

  So both $[K[\alpha] : K]$ and $[(K[\alpha])[\beta] : K[\alpha]]$ are finite.

  It follows that $[K(\alpha, \beta) : K]$ is finite.

  So, $\alpha - \beta$ is algebraic over K.

  By a similar argument, $\frac{\alpha}{\beta} \in \mathscr{A}(L)$, for all α and $\beta (\neq 0)$ in $\mathscr{A}(L)$.

The Field $\mathbb{A}$ of Algebraic Numbers

- If we take K as the field $\mathbb{Q}$ of rational numbers and L as the field $\mathbb{C}$ of complex numbers, then $\mathscr{A}(L)$ is the field $\mathbb{A}$ of **algebraic numbers**.

Theorem

The field $\mathbb{A}$ of algebraic numbers is countable.

- The proof depends on some knowledge of the arithmetic of infinite cardinal numbers. It is known that $\mathbb{Q}$ is countable. To put it in the standard notation for cardinal numbers, $|\mathbb{Q}| = \aleph_0$. Since $\mathbb{Q} \subseteq \mathbb{A}$, we know that $|\mathbb{A}| \geq \aleph_0$.

  Now, the number of monic polynomials of degree n with coefficients in $\mathbb{Q}$ is $\aleph_0^n = \aleph_0$. Each such polynomial has at most n distinct roots in $\mathbb{C}$. So the number of roots of monic polynomials of degree n is at most $n\aleph_0 = \aleph_0$. Hence, the number of roots of monic polynomials of all possible degrees is at most $\aleph_0 \cdot \aleph_0 = \aleph_0$. Thus $|\mathbb{A}| \leq \aleph_0$.

Existence of Transcendental Numbers

Theorem

Transcendental numbers exist.

- It is known that $|\mathbb{R}| = |\mathbb{C}| = 2^{\aleph_0} > \aleph_0$. It follows that $\mathbb{C} \setminus \mathbb{A}$, the set of transcendental numbers, is non-empty.
- Since $|\mathbb{C} \setminus \mathbb{A}| = 2^{\aleph_0} > |\mathbb{A}|$, we can say that "most" complex numbers are transcendental.
- This argument of Cantor was extraordinary in that it demonstrated the existence of transcendental numbers without producing a single example of such a number!
- Liouville demonstrated that $\sum_{n=1}^{\infty} \frac{1}{10^{n!}}$ is transcendental.
- Hermite proved that e is transcendental.
- Lindemann proved that π is transcendental.

Degree of an Extension and Minimum Polynomials

Theorem

Let L be an extension of F, and let the elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ of L have minimum polynomials $m_1, m_2, \ldots, m_n$, respectively, over F. Then

$$[F(\alpha_1, \alpha_2, \ldots, \alpha_n) : F] \leq \partial m_1 \partial m_2 \cdots \partial m_n.$$

- The proof is by induction on n, it being clear that $[F(\alpha_1) : F] = \partial m_1$. Suppose inductively that $[F(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}) : F] \leq \partial m_1 \partial m_2 \cdots \partial m_{n-1}$. We know that $m_n(\alpha_n) = 0$. The element α_n is certainly algebraic over $F(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})$. Its minimum polynomial over that field must have degree $\leq \partial m_n$. So $[F(\alpha_1, \alpha_2, \ldots, \alpha_n) : F(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})] \leq \partial m_n$. Now we have

$$\begin{aligned} & [F(\alpha_1, \alpha_2, \ldots, \alpha_n) : F] \\ & = [F(\alpha_1, \alpha_2, \ldots, \alpha_n) : F(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})] \cdot [F(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}) : F] \\ & \leq \partial m_1 \partial m_2 \cdots \partial m_{n-1} \partial m_n. \end{aligned}$$

Example

- We cannot assert equality in the preceding formula.
- We have

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{6}) : \mathbb{Q}] = 2,$$
$$\left[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6}) : \mathbb{Q}\right] = 4.$$

This shows that

$$\left[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6}) : \mathbb{Q}\right] < [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}][\mathbb{Q}(\sqrt{6}) : \mathbb{Q}].$$

Finite Extensions and Algebraic Elements

Proposition

An extension L of a field K is finite if and only if, for some n, there exist $\alpha_1,\alpha_2,\ldots,\alpha_n$, algebraic over K, such that $L=K(\alpha_1,\alpha_2,\ldots,\alpha_n)$.

- The theorem gives half of this result.

  Suppose now that $[L:K]$ is finite.

  Let $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ be a basis for L over K.

  The elements α_i are all algebraic.

  Then L consists of linear combinations (with coefficients in K) of $\alpha_1,\alpha_2,\ldots,\alpha_n$.

  This set contains (and is thus equal to) the seemingly larger set $K(\alpha_1,\alpha_2,\ldots,\alpha_n)$.

Subsection 3

Polynomials and Extensions

Irreducible Polynomials and Simple Algebraic Extensions

Theorem

Let K be a field and let m be a monic irreducible polynomial with coefficients in K. Then $L = K[X]/\langle m\rangle$ is a simple algebraic extension $K[\alpha]$ of K, and $\alpha = X + \langle m\rangle$ has minimum polynomial m over K.

- Let K be a field, and let $m \in K[X]$ be irreducible and monic. Let $L = K[X]/\langle m\rangle$. Then L is a field. The mapping $a \mapsto a + \langle m\rangle$ is a monomorphism from K into L. So L is an extension of K.
  Let $\alpha = X + \langle m\rangle$. Then, for $f = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ in $K[X]$,

$$\begin{array}{rcl} f(\alpha) & = & a_0 + a_1\alpha + \cdots + a_n\alpha^n \\ & = & a_0 + a_1(X + \langle m\rangle) + a_2(X + \langle m\rangle)^2 + \cdots + a_n(X + \langle m\rangle)^n \\ & = & a_0 + a_1(X + \langle m\rangle) + a_2(X^2 + \langle m\rangle) + \cdots + a_n(X^n + \langle m\rangle) \\ & = & (a_0 + a_1X + a_2X^2 + \cdots + a_nX^n) + \langle m\rangle = f + \langle m\rangle. \end{array}$$

  So $f(\alpha) = 0 + \langle m\rangle$ if and only if $m \mid f$.
  Thus, m is the minimum polynomial of α.

Isomorphisms of Extension Fields

Theorem

Let K, K' be fields, and let $\varphi : K \to K'$ be an isomorphism with canonical extension $\widehat{\varphi} : K[X] \to K'[X]$. Let $f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$ be an irreducible polynomial of degree n with coefficients in K, and let $f' = \widehat{\varphi}(f) = \varphi(a_n) X^n + \varphi(a_{n-1}) X^{n-1} + \cdots + \varphi(a_0)$. Let L be an extension of K containing a root α of f, and let L' be an extension of K' containing a root α' of f'. Then there is an isomorphism ψ from $K[\alpha]$ onto $K'[\alpha']$, extending φ.

- The field $K[\alpha]$ consists of polynomials $b_0 + b_1 \alpha + \cdots + b_{n-1} \alpha^{n-1}$. Addition is obvious. Multiplication is carried out using the equation $\alpha^n = -\frac{1}{a_n}(a_{n-1}\alpha^{n-1} + \cdots + a_0)$. The mapping ψ is defined by

$$\psi(b_0 + b_1 \alpha + \cdots + b_{n-1} \alpha^{n-1}) = \varphi(b_0) + \varphi(b_1)\alpha' + \cdots + \varphi(b_{n-1}) \alpha'^{n-1}.$$

More compactly, $\psi(u(\alpha)) = (\widehat{\varphi}(u))(\alpha')$, for all u in $K[X]$ with $\partial u < n$.

Isomorphisms of Extension Fields (Cont'd)

- ψ is onto. This follows by observing that:
  - $K'[\alpha']$ consists of polynomials of the form $b'_0 + b'_1\alpha' + \cdots + b'_{n-1}\alpha'^{n-1}$, with $b'_0, \ldots, b'_{n-1}$ in K';
  - $\varphi : K \to K'$ is onto.
- ψ is one-to-one: We have

$$\psi(b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}) = \psi(c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1})$$
$$\varphi(b_0) + \varphi(b_1)\alpha' + \cdots + \varphi(b_{n-1})\alpha'^{n-1} = \varphi(c_0) + \varphi(c_1)\alpha' + \cdots + \varphi(c_{n-1})\alpha'^{n-1}$$
$$(\varphi(b_0) - \varphi(c_0)) + (\varphi(b_1) - \varphi(c_1))\alpha' + \cdots + (\varphi(b_{n-1}) - \varphi(c_{n-1}))\alpha'^{n-1} = 0.$$

  Since $[K'[\alpha'] : K'] = n$, the polynomial on the left must be zero.

  So we get $\varphi(b_0) = \varphi(c_0), \varphi(b_1) = \varphi(c_1), \ldots, \varphi(b_{n-1}) = \varphi(c_{n-1})$.

  As ϕ is one-to-one, $b_0 = c_0, b_1 = c_1, \ldots, b_{n-1} = c_{n-1}$.

  Therefore, ψ is one-to-one.
- That ψ extends ϕ is clear.

Isomorphisms of Extension Fields (Conclusion)

- From the definition of ψ it is also clear that $\psi(u(\alpha)+v(\alpha))=\psi(u(\alpha))+\psi(v(\alpha))$.
- In multiplying $u(\alpha)$ and $v(\alpha)$, we use the minimum polynomial to reduce the answer to the form $w(\alpha)$, $\partial w \leq n-1$.

  We use the division algorithm to write $uv=qm+w$, where $\partial w < n$.

  Hence $\psi(u(\alpha)v(\alpha))=\psi(w(\alpha))=(\widehat{\varphi}(w))(\alpha')$.

  The isomorphism $\widehat{\varphi}$ implies that the division algorithm in $K'[X]$ gives $\widehat{\varphi}(u)\widehat{\varphi}(v)=\widehat{\varphi}(q)\widehat{\varphi}(m)+\widehat{\varphi}(w)$. Hence,

$$
\begin{aligned}
(\psi(u(\alpha))\psi(v(\alpha)) &= (\widehat{\varphi}(u))(\alpha')(\widehat{\varphi}(v))(\alpha') \\
&= (\widehat{\varphi}(u)\widehat{\varphi}(v))(\alpha') \\
&= (\widehat{\varphi}(q)\widehat{\varphi}(m)+\widehat{\varphi}(w))(\alpha') \\
&= (\widehat{\varphi}(q))(\alpha')(\widehat{\varphi}(m))(\alpha')+(\widehat{\varphi}(w))(\alpha') \\
&= (\widehat{\varphi}(w))(\alpha') \\
&= \psi(u(\alpha)v(\alpha)).
\end{aligned}
$$

K-Isomorphisms

Corollary

Let K be a field, and let f be an irreducible polynomial with coefficients in K. If L, L' are extensions of K containing roots α, α' of f, respectively, then there is an isomorphism from $K[\alpha]$ onto $K[\alpha']$ which fixes every element of K.

- An isomorphism α from L onto L' with the property that

$$\alpha(x) = x, \text{ for every element } x \text{ of } K,$$

i.e., that fixes every element of K, is called a K-**isomorphism**.

Example

- If $K = \mathbb{R}$ and $m = X^2 + 1$, the field $L = K[X]/\langle X^2 + 1\rangle$ contains an element $\delta = X + \langle X^2 + 1\rangle$, such that $\delta^2 = -1$.

  The polynomial $X^2 + 1$ is irreducible over $\mathbb{R}$.

  It factorizes into $(X + \delta)(X - \delta)$ in the field L.

  Every element of L can be uniquely expressed in the form $a + b\delta$.

  So L is none other than the field $\mathbb{C}$ of complex numbers.
- By the Fundamental Theorem of Algebra every polynomial with coefficients in $\mathbb{C}$ factorizes into linear factors.

  So every irreducible m in $\mathbb{Q}[X]$ factorizes completely in $\mathbb{C}[X]$.

  If we know the factors, it is easier to deal, e.g., with the subfield $\mathbb{Q}[i\sqrt{3}] = \{a + bi\sqrt{3} : a, b \in \mathbb{Q}\}$ of $\mathbb{C}$ than with $\mathbb{Q}[X]/\langle X^2 + 3\rangle$.

  The two fields are, of course, isomorphic to each other.

Example

- The polynomial $m = X^2 + X + 1$ is irreducible over $\mathbb{Z}_2$.
  Any proper factor would be either $X - 0$ or $X - 1$, and neither 0 nor 1 is a root of m.
  We form the field $L = \mathbb{Z}_2[X]/\langle m \rangle$.
  It has 4 elements, namely,
  $$0 + \langle m \rangle,\ 1 + \langle m \rangle,\ X + \langle m \rangle,\ 1 + X + \langle m \rangle.$$
  We write them as $0, 1, \alpha$ and $1 + \alpha$, where $\alpha^2 + \alpha + 1 = 0$.
  The addition and multiplication in L are given by

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$\cdot$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

Example

- We show that $\varphi : \mathbb{Q}[i+\sqrt{2}] \to \mathbb{Q}[X]/\langle X^4 - 2X^2 + 9\rangle$, defined by
$$\varphi(a) = a + \langle X^4 - 2X^2 + 9\rangle,\ a \in \mathbb{Q},\ \varphi(i+\sqrt{2}) = X + \langle X^4 - 2X^2 + 9\rangle,$$
is an isomorphism. Then, we determine $\varphi(i)$.
It is clear that $[\mathbb{Q}[i+\sqrt{2}] : Q] = 4$.
We compute
$$\begin{aligned}(i+\sqrt{2})^2 &= i^2 + 2i\sqrt{2} + 2 = 1 + 2i\sqrt{2};\\ (i+\sqrt{2})^4 &= (1+2i\sqrt{2})^2 = 1 + 4i\sqrt{2} - 8 = -7 + 4i\sqrt{2}.\end{aligned}$$
We verify
$$(i+\sqrt{2})^4 - 2(i+\sqrt{2})^2 + 9 = -7 + 4i\sqrt{2} - 2 - 4i\sqrt{2} + 9 = 0.$$
So the minimum polynomial of $i+\sqrt{2}$ over $\mathbb{Q}$ is $X^4 - 2X^2 + 9$.
By uniqueness φ is an isomorphism.

Example (Cont'd)

- Let $a_0, \ldots, a_3 \in \mathbb{Q}$.
  Observe that

$$\begin{aligned} & a_0 + a_1(i+\sqrt{2}) + a_2(i+\sqrt{2})^2 + a_3(i+\sqrt{2})^3 \\ &= a_0 + a_1(i+\sqrt{2}) + a_2(1+2i\sqrt{2}) + a_3(5i-\sqrt{2}) \\ &= (a_0+a_2) + (a_1+5a_3)i + (a_1-a_3)\sqrt{2} + (2a_2)i\sqrt{2}. \end{aligned}$$

  Since $\{1, i, \sqrt{2}, i\sqrt{2}\}$ is linearly independent over $\mathbb{Q}$, this equals i if and only if

$$\left\{ \begin{array}{rcl} a_0+a_2 & = & 0 \\ a_1+5a_3 & = & 1 \\ a_1-a_3 & = & 0 \\ a_2 & = & 0 \end{array} \right\} \Rightarrow \left\{ \begin{array}{lcl} a_0 & = & 0 \\ a_1 & = & \frac{1}{6} \\ a_2 & = & 0 \\ a_3 & = & \frac{1}{6} \end{array} \right.$$

  Thus, $i = \frac{1}{6}((i+\sqrt{2}) + (i+\sqrt{2})^3)$.
  So $\varphi(i) = \frac{1}{6}(X+X^3) + \langle X^4 - 2X^2 + 9 \rangle$.