Field extensions

Nicolas Mascot

TCD

March 13, 2020

Context

Let K and L be fields such that $K \subseteq L$. One says that K is a subfield of L, and that L is an extension of K.

Example

$\mathbb{R}$ is a subfield of $\mathbb{C}$, and $\mathbb{C}$ is an extension of $\mathbb{R}$.

Notation

In what follows, whenever $\alpha \in L$, we write $K(\alpha)$ for the subfield of L generated by K and α, and $K[\alpha]$ for the subring of L generated by K and α.

Example

The ring $K[\alpha]$ is a subring of the field $K(\alpha)$.

Example

$\mathbb{C} = \mathbb{R}(i) = \mathbb{R}[i]$.

We have

$$K[\alpha] = \{P(\alpha),\ P(x) \in K[x]\}.$$

For $K(\alpha)$, more delicate, as we will see below.

Algebraic vs. transcendental (1/2)

Definition

Let $K \subset L$, and let $\alpha \in L$. Then

$$I_\alpha = \{F(x) \in K[x] \mid F(\alpha) = 0\}$$

is an ideal of $K[x]$. One says that α is algebraic over K if this ideal is nonzero, that is to say if there exists a nonzero $F(x) \in K[x]$ which vanishes at α. Else one says that α is transcendental over K.

Example

$\alpha = i \in \mathbb{C}$ is algebraic over $\mathbb{R}$, since it is a root of the nonzero polynomial $P(x) = x^2 + 1 \in \mathbb{R}[x]$. In fact, α is even algebraic over $\mathbb{Q}$ since $P(x) \in \mathbb{Q}[x]$.

Algebraic vs. transcendental (2/2)

Counter-example

One can show (but this is difficult) that π is transcendental over $\mathbb{Q}$. This means for instance that an "identity" of the form

$$2130241\pi^3 - 22294338\pi^2 + 51516201\pi - 7857464 = 0$$

is automatically **FALSE**.
On the other hand, π is algebraic over $\mathbb{R}$, since it is a root of $x - \pi \in \mathbb{R}[x]$.

Definition

If every element of L is algebraic over K, one says that L is an <u>*algebraic extension*</u> *of K.*

Minimal polynomials (1/2)

Since since the ring $K[x]$ is a PID, the ideal I_α is principal, so there exists a polynomial $M(x) \in K[x]$ such that

$$I_\alpha = \big(M(x)\big) = M(x)K[x].$$

If α is transcendental over K, then $I_\alpha = \{0\}$ so $M(x)$ is the zero polynomial.
Suppose on the contrary that α is algebraic over K, so that $M(x) \neq 0$. Since $K[x]$ is a domain, the other generators of I_α are the associates of $M(x)$ in $K[x]$, that is the $U(x)M(x)$ for $U \in K[x]^\times$. But $K[x]^\times = K^\times$, so $M(x)$ is unique up to scaling, so there is a unique monic polynomial $m_\alpha(x)$ that generates I_α.

Definition

$m_\alpha(x)$ is called the minimal polynomial of α over K.

Minimal polynomials (2/2)

Definition

One then says that α is algebraic over K of degree n, where $n = \deg m_\alpha \in \mathbb{N}$, and one writes $\deg_K \alpha = n$.

Remark

By definition, for all $F(x) \in K[x]$, $F(\alpha) = 0 \iff F$ is a multiple of m_α. In particular, m_α is the unique (up to scaling) polynomial of minimal degree vanishing at $x = \alpha$, hence the name minimal polynomial.

Minimal polynomials and irreducibility

Remark

Minimal polynomials (over a field K) are always irreducible (over the same field K). Indeed, let $m_\alpha(x) \in K[x]$ be the minimal polynomial of some $\alpha \in L$, and suppose $m_\alpha(x) = A(x)B(x)$ with $A(x), B(x) \in K[x]$. Then $0 = m_\alpha(\alpha) = A(\alpha)B(\alpha)$, so WLOG we may assume that $A(\alpha) = 0$. By definition of the minimal polynomial, $m_\alpha(x) \mid A(x)$; but also $A(x) \mid m_\alpha(x)$, so A and m_α must be associate, so $B(x)$ must be a constant as $K[x]^\times = K^\times$.

Remark

Conversely, if $M(x) \in K[x]$ vanishes at $x = \alpha$ and it monic and irreducible, then $M(x)$ is the minimal polynomial of α. Indeed, $M(\alpha) = 0$ implies $m_\alpha \mid M$, and since both are irreducible, they must be associate, hence equal since they are both monic.

Minimal polynomials: examples (1/2)

Example

Let $K = \mathbb{Q}$, $L = \mathbb{C}$, and $\alpha = \sqrt[3]{2} \in L$. Then α is a root of $M(x) = x^3 - 2$, so α is algebraic over $\mathbb{Q}$. Besides, $M(x)$ is monic and irreducible over $\mathbb{Q}$ because it is Eisenstein at $p = 2$, so $M(x)$ is the minimal polynomial of α over $\mathbb{Q}$, so

$$I_\alpha = (x^3 - 2),$$

which means an element of $K[x]$ vanishes at α iff. it is divisible by $M(x)$. In particular, we have

$$\deg_{\mathbb{Q}} \alpha = \deg M = 3.$$

However, the minimal polynomial of α over $\mathbb{R}$ is **NOT** $M(x)$, but $x - \alpha \in \mathbb{R}[x]$.

Minimal polynomials: examples (2/2)

Example

Let $K = \mathbb{Q}$, $L = \mathbb{C}$, and $\alpha = e^{2\pi i/3}$ so that $\alpha^3 = 1$. Then α is a root of

$$M(x) = x^3 - 1 \in K[x],$$

so α is algebraic over K (of degree at most 3, since its minimal polynomial must divide M). However,

$$M(x) = (x-1)(x^2+x+1) \in K[x]$$

is not irreducible over K, so it is **NOT** the minimal polynomial of α over K. In fact, since $\alpha - 1 \neq 0$, α is a root of the cofactor

$$N(x) = x^2 + x + 1 \in K[x].$$

This cofactor is irreducible over K, so it is the minimal polynomial of α over K, and $\deg_K \alpha = 2$.

The degree of an extension

Let L be an extension of a field K. If we forget temporarily about the multiplication on L, so that only addition is left, then L can be seen as a vector space over K.

Definition

The degree of L over K is the dimension (finite or infinite) of L seen as a K-vector space. It is denoted by $[L : K]$.
If this degree is finite, one says that L is a finite extension of K.

Example

$\mathbb{C}$ is an extension of $\mathbb{R}$, so $\mathbb{C}$ is a vector space over $\mathbb{R}$. In fact, it admits $\{1, i\}$ are a basis, so it has finite dimension, namely 2, so $\mathbb{C}$ is a finite extension of $\mathbb{R}$, of degree

$$[\mathbb{C} : \mathbb{R}] = 2.$$

Extension degree vs. algebraic degree

Theorem

Let $K \subset L$ be a field extension, and let $\alpha \in L$.

1. *If α is transcendental over K, then evaluating at $x = \alpha$ yields a ring isomorphism $K[x] \simeq K[\alpha]$ and a field isomorphism $K(x) \simeq K(\alpha)$. In particular, $K(\alpha)$ is an infinite extension of K.*
2. *If α is algebraic over K of degree n, then $K[\alpha]$ is a field, so it agrees with $K(\alpha)$. It is also a vector space of dimension n over K, with basis $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$. In particular, $K(\alpha)$ is a finite extension of K, of degree*
$$[K(\alpha) : K] = n.$$

Extension degree vs. algebraic degree, proof (1/3)

Proof, case α transcendental over K

$$\begin{array}{ccc} K[x] & \longrightarrow & K[\alpha] \\ P(x) & \longmapsto & P(\alpha) \end{array}$$

is a ring morphism, is surjective by definition of $K[\alpha]$, and injective: if $P(x)$ lies in the kernel, then $P(\alpha) = 0$, so $P(x)$ is the 0 polynomial as α is transcendental.

This extends into the field morphism

$$\begin{array}{ccc} K(x) & \longrightarrow & K(\alpha) \\ \dfrac{P(x)}{Q(x)} & \longmapsto & \dfrac{P(\alpha)}{Q(\alpha)} \end{array}$$

which is well defined since $Q(\alpha) \neq 0$ for nonzero $Q(x)$, surjective by definition of $K(\alpha)$, and injective by the same reason as above.

In particular, $1 = \alpha^0, \alpha, \alpha^2, \alpha^3, \cdots \in K(\alpha)$ are linearly independent over K, so $[K(\alpha) : K] = +\infty$.

Extension degree vs. algebraic degree, proof (2/3)

Proof, case α algebraic over K

Let us begin by proving that $1, \alpha, \cdots, \alpha^{n-1}$ is a K-basis of $K[\alpha]$. Let $m(x) = m_\alpha(x) \in K[x]$ be the minimal polynomial of α over K; it has degree n. For all $P(x) \in K[x]$, we may perform the Euclidean division

$$P(x) = m(x)Q(x) + R(x)$$

where $Q(x), R(x) \in K[x]$ and $\deg R(x) < n$. Evaluating at $x = \alpha$, we find that $P(\alpha) = R(\alpha)$, so every element of $K[\alpha]$ is of the form $\sum_{j=0}^{n-1} \lambda_j \alpha^j$ for some $\lambda_j \in K$. Besides, if we had a relation of the form $\sum_{j=0}^{n-1} \lambda_j \alpha^j = 0$ with the λ_j in K and not all zero, this would mean that the nonzero polynomial $\sum_{j=0}^{n-1} \lambda_j x^j \in K[x]$ of degree $< n$ vanishes at $x = \alpha$, which contradicts the definition of the minimal polynomial.
Therefore, $1, \alpha, \cdots, \alpha^{n-1}$ is a K-basis of $K[\alpha]$. Since there are n of them, we have $[K(\alpha) : K] = n$.

Extension degree vs. algebraic degree, proof (3/3)

Proof, case α algebraic over K

We must now prove that the ring $K[\alpha]$ is actually a field. Let us thus prove that any nonzero $\beta \in K[\alpha]$ is invertible in $K[\alpha]$. We know from the above that $\beta = P(\alpha)$ for some nonzero $P(x) \in K[x]$ of degree $< n$. Since $m(x)$ is irreducible over K and $\deg P(x) < \deg m(x) = n$, it follows that $P(x)$ and $m(x)$ are coprime, so that there exist $U(x)$ and $V(x)$ in $K[x]$ such that

$$U(x)P(x) + V(x)m(x) = 1.$$

Evaluating at $x = \alpha$, we find that $U(\alpha)P(\alpha) + 0 = 1$, which proves that $U(\alpha) \in K[\alpha]$ is the inverse of $\beta = P(\alpha)$. $\square$

Extension degree vs. algebraic degree, examples

Example

Let $\alpha = \sqrt[3]{2}$. We have seen that the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $x^3 - 2$, so $\deg_{\mathbb{Q}} \sqrt[3]{2} = 3$. As a result,

$$\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q} \oplus \mathbb{Q}\sqrt[3]{2} \oplus \mathbb{Q}\sqrt[3]{2}^2,$$

which means that every element of $\mathbb{Q}(\sqrt[3]{2})$ can be written in a unique way as $a + b\sqrt[3]{2} + c\sqrt[3]{2}^2$ with $a, b, c \in \mathbb{Q}$.

Extension degree vs. algebraic degree, examples

Example

Similarly, since $i^2 = -1$, i is algebraic of degree 2 over $\mathbb{Q}$, with minimal polynomial $x^2 + 1$. It is also algebraic of degree 2 over $\mathbb{R}$, with the same minimal polynomial $x^2 + 1$, but which is this time seen as lying in $\mathbb{R}[x]$. We deduce that

$$\mathbb{Q}(i) = \mathbb{Q}[i] = \mathbb{Q} \oplus \mathbb{Q}i$$

and that

$$\mathbb{C} = \mathbb{R}(i) = \mathbb{R}[i] = \mathbb{R} \oplus \mathbb{R}i.$$

We thus recover the well-known fact that every complex number can be written uniquely as $a + bi$ with $a, b \in \mathbb{R}$. We also get that the elements of $\mathbb{Q}(i)$ may be written uniquely as $a + bi$ with $a, b \in \mathbb{Q}$; in particular, these elements form a subfield of $\mathbb{C}$.

Extension degree vs. algebraic degree, examples

Example

On the contrary, since π is transcendental over $\mathbb{Q}$, $\mathbb{R}$ is not an algebraic extension of $\mathbb{Q}$, and its subfield $\mathbb{Q}(\pi)$ is isomorphic to $\mathbb{Q}(x)$ by $x \mapsto \pi$.

Extension degree vs. algebraic degree, examples

Example

Finally, one can prove that $\sqrt{3}$ is algebraic of degree 2 over $\mathbb{Q}(\sqrt{2})$. This amounts to say that x^2-3, which is irreducible over $\mathbb{Q}$, remains irreducible over $\mathbb{Q}(\sqrt{2})$. Indeed, if it became reducible, then $\sqrt{3}$ would lie in $\mathbb{Q}(\sqrt{2})$. Since $(1, \sqrt{2})$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt{2})$, there would exist $a, b \in \mathbb{Q}$ such that $\sqrt{3} = a + b\sqrt{2}$. Squaring yields $3 = (a^2+2b^2) + 2ab\sqrt{2}$, which implies that $a^2+2b^2 = 3$ and that $2ab = 0$, which is clearly impossible. So

$$\mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2}) \oplus \mathbb{Q}(\sqrt{2})\sqrt{3}$$

as a vector space over $\mathbb{Q}(\sqrt{2})$, so that every element of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ can be written in a unique way as $a + b\sqrt{3}$ with $a, b \in \mathbb{Q}(\sqrt{2})$.

A converse

Theorem

If an extension is finite, then it is algebraic.

Proof.

Let $n = [L : K] < +\infty$, and let $\alpha \in L$. The $n+1$ vectors

$$1 = \alpha^0, \alpha, \alpha^2, \cdots, \alpha^n$$

lie in the vector space L of dimension n, so they must be linearly dependent. This means we have

$$\lambda_0 1 + \lambda_1 \alpha + \lambda_2 \alpha^2 + \cdots + \lambda_n \alpha^n = 0$$

for some $\lambda_i \in K$ not all 0, which proves that α is algebraic over K. □

A converse

Example

Let L be an extension of K, and $\alpha \in L$ be algebraic over K. Then $K(\alpha)$ is a finite extension of K, so it is an algebraic extension of K, so that all its elements (such that α^2) are also algebraic over K.

Counter-example

The converse is false: there exist extensions that are algebraic, but not finite. More below.

The tower law

Theorem (Tower law)

Let $K \subseteq L \subseteq M$ be finite extensions, let

$$(l_i)_{1 \leqslant i \leqslant [L:K]}$$

be a K-basis of L, and let

$$(m_j)_{1 \leqslant j \leqslant [M:L]}$$

be an L-basis of M. Then

$$(l_i m_j)_{\substack{1 \leqslant i \leqslant [L:K] \\ 1 \leqslant j \leqslant [M:L]}}$$

is a K-basis of M.

In particular, $[M : K] = [M : L][L : K]$.

The tower law, proof (1/2)

Proof : Generating

Let $m \in M$. Since $(m_j)_{1 \leqslant j \leqslant [M:L]}$ is an L-basis of M, we have

$$m = \sum_{j=1}^{[M:L]} \lambda_j m_j$$

for some $\lambda_j \in L$, and since $(l_i)_{1 \leqslant i \leqslant [L:K]}$ is a K-basis of L, each λ_j can be written

$$\lambda_j = \sum_{i=1}^{[L:K]} \mu_{i,j} l_i.$$

Thus we have

$$m = \sum_{j=1}^{[M:L]} \sum_{i=1}^{[L:K]} \mu_{i,j} l_i m_j,$$

which proves that the $l_i m_j$ span M over K.

The tower law, proof (2/2)

Proof: Independent

Suppose now that

$$\sum_{j=1}^{[M:L]} \sum_{i=1}^{[L:K]} \mu_{i,j} l_i m_j = 0$$

with $\mu_{i,j} \in K$. This can be written as

$$\sum_{j=1}^{[M:L]} \lambda_j m_j = 0, \text{ where } \lambda_j = \sum_{i=1}^{[L:K]} \mu_{i,j} l_i \in L.$$

Since $(m_j)_{1 \leqslant j \leqslant [M:L]}$ is an L-basis of M, this would imply that each of the λ_j is 0. And since $(l_i)_{1 \leqslant i \leqslant [L:K]}$ is a K-basis of L, this means that the $\mu_{i,j}$ are all zero. Thus the $l_i m_j$ are linearly independent over K. □

The tower law, example

Example

We have seen above that

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \text{ and } [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2.$$

It then follows from the tower law that

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

More precisely, since we know that $(1, \sqrt{2})$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt{2})$, and that $(1, \sqrt{3})$ is a $\mathbb{Q}(\sqrt{2})$-basis of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, we deduce from the tower law that $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. This means that each element of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ may be written as $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ for unique $a, b, c, d \in \mathbb{Q}$.

Algebraicness is preserved by field operations

Theorem

Let L/K be a field extension. The sum, difference, product, and quotient of two elements of L which are algebraic over K are algebraic over K.

Algebraicness is preserved by field operations

Proof.

Let $\alpha, \beta \in L$; note that $K(\alpha, \beta) = K(\alpha)(\beta)$. If α is algebraic over K, then we have $[K(\alpha) : K] < +\infty$. If furthermore β is also algebraic over K, then it satisfies a non-trivial equation in $K[x]$; viewing this equation as an element of $K(\alpha)[x]$, we deduce that β is also algebraic over $K(\alpha)$, so that $[K(\alpha)(\beta) : K(\alpha)] < +\infty$. The tower law then yields

$$[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\alpha)][K(\alpha) : K] < +\infty,$$

in other words $K(\alpha, \beta)$ is a finite extension of K. It is thus an algebraic extension of K. which means that all its elements, including $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$, and α/β (if $\beta \neq 0$) are algebraic over K. □

Algebraicness is preserved by field operations

Example

Let

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ algebraic over } \mathbb{Q}\}.$$

By the above, $\overline{\mathbb{Q}}$ is actually a subfield of $\mathbb{C}$. Besides, $\overline{\mathbb{Q}}$ is by definition an algebraic extension of $\mathbb{Q}$. However, it it is not a finite one. Indeed, one can show that in the chain

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) \subseteq \cdots$$

(throw in the square root of each prime number one by one), each extension is of degree 2, so that the *n*-th extension is of degree 2^n over $\mathbb{Q}$ by the tower law, which forces $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$. We thus have an example of an extenson which is algebraic, but not finite.

Constructible numbers (1/6)

Suppose we are given an orthonormal coordinate frame (O, I, J) in the plane. A point is said to be constructible if we can obtain it from O, I, J in finitely many steps using only a ruler and a compass. A number $\alpha \in \mathbb{R}$ is said to be constructible if it is a coordinate of a constructible point; equivalently, α is constructible if $|\alpha|$ is the distance between two constructible points.

A bit of geometry shows that the set of constructible numbers is a subfield of $\mathbb{R}$, which is stable under radicals (of positive elements only, of course).

Constructible numbers (2/6)

Conversely, suppose that we perform a ruler-and-compass construction in $n \in \mathbb{N}$ steps, and let K_j ($j \leq n$) be the subfield of $\mathbb{R}$ generated by the coordinates of the points constructed at the j-th step, so that $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$. At each step j, we either construct the intersection of two lines, or the intersection of a line and a circle or of two circles. In the first case, the coordinates of the intersection can be found by solving a linear system, which can be done by field operations in K_j, so that $K_{j+1} = K_j$. In the second case, the coordinates of the intersection can be found by solving quadratic equations, so that $[K_{j+1} : K_j]$ is either 1 (if the solutions to these equations already lie in K_j) or 2 (if they do not, so that K_{j+1} is genuinely bigger than K_j). By removing the steps such that $K_{j+1} = K_j$, we thus establish the following result:

Constructible numbers (3/6)

Theorem (Wantzel)

Let $\alpha \in \mathbb{R}$. Then α is constructible iff. there exist fields

$$\mathbb{Q} = K_0 \subsetneq K_1 \subsetneq \cdots \subsetneq K_n$$

such that $[K_{j+1} : K_j] = 2$ for all j and that $\alpha \in K_n$.

Constructible numbers (4/6)

Corollary

If $\alpha \in \mathbb{R}$ is constructible, then α is algebraic over $\mathbb{Q}$, and $\deg_{\mathbb{Q}} \alpha$ is a power of 2.

Proof.

Since α is constructible, there exist fields

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n \ni \alpha$$

such that $[K_{j+1} : K_j] = 2$ for all j. By the tower law, we have $[K_j : \mathbb{Q}] = 2^j$ for all j, so in particular $[K_n : \mathbb{Q}] = 2^n$. It follows that K_n is a finite, and therefore algebraic, extension of $\mathbb{Q}$, so α is algebraic over $\mathbb{Q}$. Besides, $\deg_{\mathbb{Q}}(\alpha) = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \frac{[K_n:\mathbb{Q}]}{[K_n:\mathbb{Q}(\alpha)]}$ divides $[K_n : \mathbb{Q}] = 2^n$, so it is also a power of 2. □

Constructible numbers (5/6)

Example

Since π is transcendental over $\mathbb{Q}$, is is not constructible. This shows that squaring the circle is impossible.

Example

We have seen that $\sqrt[3]{2}$ is algebraic of degree 3 over $\mathbb{Q}$. Since 3 is not a power of 2, $\sqrt[3]{2}$ is not constructible.

Constructible numbers (6/6)

Remark

Beware that the converse to the corollary is false! For instance, the polynomial $x^4 - 8x^2 + 4x + 2$ is irreducible over $\mathbb{Q}$ since it is Eisenstein at 2, and is therefore the minimal polynomial of each of its roots over $\mathbb{Q}$, so that these roots are algebraic of degree 4 over $\mathbb{Q}$. It happens that these roots are all real, but that none of them is constructible!
The problem is that if α is such a root, then we do have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, but this does not imply the existence of an intermediate field K such that $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\alpha)$ where both intermediate extensions are of degree 2, i.e. the hypotheses of Wantzel's theorem are not necessarily satisfied (and in fact they are not).