Abstract Algebra, Lecture 14

Field extensions

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet

Linköping, fall 2019

Lecture notes availabe at course homepage
http://courses.mai.liu.se/GU/TATA55/

Summary

Summary

Summary

Summary

Definition

Suppose that E, F are fields, and that E is a subring of F. We write $E \leq F$ and say that E is a subfield of F, and that F is an overfield of E. The inclusion map $i : E \to F$ is called a field extension (or equivalently, the pair $E \leq F$).

Example

- Any field is an overfield of its prime subfield
- $\mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$
- $\mathbb{C} \leq \mathbb{C}(x) \leq \mathbb{C}(x)(y)$
- $\mathbb{Z}_2 \leq \frac{\mathbb{Z}_2[x]}{(x^2+x+1)}$

Definition

Let $E \leq F$ be a field extension. Then F is a vector space over E. The dimension is denoted by $[F : E]$, and refered to as the degree of the extension. If this dimension is finite, then the extension is said to be finite dimensional.

Example

- $[\mathbb{C} : \mathbb{R}] = 2$, so $\mathbb{R} \leq \mathbb{C}$ is a finite dimensional extension of degree 2.
- $[\mathbb{R} : \mathbb{Q}] = \infty$, so this extension is infinite dimensional.

It is a theorem (as long as you accept the axiom of choice) that any vector space has a basis. In the first example, we can take $\{1, i\}$, in the second, we need set-theory yoga to produce a *Hamel basis*.

Theorem (Tower thm)

If $K \leq L \leq M$, then $[M:K] = [M:L][L:M]$.

Proof

Obvious if any extension involved is infinite, so suppose $[M:L] = m < \infty$, $[L:K] = n < \infty$. Then M has an L-basis

$$\mathtt{u}_1, \ldots, \mathtt{u}_m,$$

and L has a K-basis

$$\mathtt{v}_1, \ldots, \mathtt{v}_n.$$

Claim:

$$\mathtt{u}_i \mathtt{v}_j, \qquad 1 \leq i \leq m, 1 \leq j \leq n$$

is a K-basis for M.

Proof (of claim)

Spanning: take $\mathtt{w} \in M$. Then

$$
\begin{aligned}
\mathtt{w} &= \sum_{i=1}^{m} c_i \mathtt{u}_i, \qquad c_i \in L \\
&= \sum_{i=1}^{m} \left(\sum_{j=1}^{n} d_{ij} \mathtt{v}_j \right) \mathtt{u}_i, \qquad d_{ij} \in K \\
&= \sum_{i,j} d_{ij} \mathtt{v}_j \mathtt{u}_i
\end{aligned}
$$

Proof (of claim)

K-linear independence: suppose that

$$\sum_{i,j} d_{ij} \mathtt{v}_j \mathtt{u}_i = 0.$$

Then

$$\sum_{i=1}^{m} \left(\sum_{j=1}^{n} d_{ij} \mathtt{v}_j \right) \mathtt{u}_i = 0,$$

so since the $\mathtt{u}_i$'s are L-linearly independent, all coefficients

$$\sum_{j=1}^{n} d_{ij} \mathtt{v}_j = 0.$$

But the $\mathtt{v}_j$'s are K-linearly independent, so all d_{ij}'s are zero.

□

Example

$$\mathbb{Z}_2 \leq \frac{\mathbb{Z}_2[x]}{(x^2+x+1)} \leq \frac{\left(\frac{\mathbb{Z}_2[x]}{(x^2+x+1)}\right)[y]}{(y^3+y+1)}$$

has degree $3 * 2 = 6$, and a basis consists of

$$1, \overline{x}, \overline{y}, \overline{xy}, \overline{y^2}, \overline{xy^2}.$$

This finite field thus has $2^6 = 64$ elements.

Definition

If $E \leq F$, $u \in F$ is algebraic over E if there is a non-zero polynomial $f(x) \in E[x]$ having u has a zero, i.e.,

$$f(x) = \sum_{i=0}^{n} a_i x^i, \qquad a_i \in E,$$

and

$$f(u) = \sum_{i=0}^{n} a_i u^i = 0 \in F.$$

The smallest degree of a polynomial that works is the degree of u over E. If u is not algebraic over E, then it is transcendental over E.

Example

$s = \sqrt{2} + 1 \in \mathbb{R}$ is algebraic of degree 2 over $\mathbb{Q}$, since it satisfies

$$(s-1)^2 - 2 = 0,$$

but no non-trivial algebraic relation of lower degree.

On the other hand, the number

$$\sum_{j=1}^{\infty} 10^{-j!}$$

is transcendental over $\mathbb{Q}$, as proved by Liouville.

Definition

The extension $E \leq F$ is algebraic if every $u \in F$ is algebraic over E.

Example

Let $E = \mathbb{Q}$, and let $F = \left\{ a + b\sqrt{2} \middle| a, b \in \mathbb{Q} \right\}$. Put $u = a + b\sqrt{2}$.

- F is a field, since

$$u^{-1} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 + 2b^2} = \frac{a}{a^2 + 2b^2} + \frac{-b}{a^2 + 2b^2}\sqrt{2}.$$

  Note that $a^2 + 2b^2 \neq 0$ when $(0,0) \neq (a,b) \in \mathbb{Q} \times \mathbb{Q}$.
- $E \leq F$
- $E \leq F$ is algebraic, with every element of F algebraic over $\mathbb{Q}$ with degree at most 2, since

$$(u - a)^2 - 2b^2 = 0.$$

Theorem

If $[F : E] = n < \infty$ then $E \leq F$ is algebraic.

Proof.

Take $u \in F$, and consider

$$1, u, u^2, \dots, u^n \in F$$

These $n+1$ vectors must be linearly dependent over E, which means that there are $c_i \in E$, not all zero, such that

$$c_0 1 + c_1 u + \cdots + c_n u^n = 0$$

Thus, u is algebraic over E. $\square$

Example

There are algebraic extensions that are not finite-dimensional. For instance, let $E = \mathbb{Q}$, and let F be the smallest subfield of $\mathbb{R}$ that contains all $\sqrt{p}$ for all primes p. Then all elements of F are algebraic; for instance, if $u = \sqrt{2} + \frac{7}{12}\sqrt{3}$ then

$$
\begin{aligned}
(u - \sqrt{2})^2 &= \frac{3 * 49}{12^2} = \frac{49}{48} \\
u^2 - 2\sqrt{2}u + 2 - \frac{49}{48} &= 0 \\
2\sqrt{2}u &= u^2 + (2 - \frac{49}{48}) = u^2 + \frac{47}{48} \\
8u &= (u^2 + \frac{47}{48})^2
\end{aligned}
$$

But the set $\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots$ is infinite and $\mathbb{Q}$-linearly independent, so $[F : E] = \infty$.

Definition

Let $E \leq F$ be a field extension, and let $u \in F$. We denote by $E(u)$ the smallest subfield of F containing E and u, in other words

$$E(u) = \bigcap_{\substack{E \leq K \leq F \\ u \in K}} K$$

Picture!

We can also describe it as

$$E(u) = \left\{ \frac{p(u)}{q(u)} \middle| p(x), q(x) \in E[x], \; q(x) \neq z.p \right\}$$

We call $E(u)$ a *simple extension*, and u a *primitive element* of the extension.

Example

$\mathbb{Q}(\sqrt{2})$ consists of all rational expressions like

$$\frac{a_0 + a_1\sqrt{2} + a_2\sqrt{2}^2 + \cdots + a_n\sqrt{2}^n}{b_0 + b_1\sqrt{2} + b_2\sqrt{2}^2 + \cdots + b_m\sqrt{2}^m},$$

but this actually simplifies to just all

$$a_0 + a_1\sqrt{2}.$$

On the other hand, put $u = \sum_{j=1}^{\infty} 10^{-j!}$, then all expressions

$$\frac{a_0 + a_1 u + a_2 u^2 + \cdots + a_n u^n}{b_0 + b_1 u + b_2 u^2 + \cdots + b_m u^m},$$

that are not identical, are different. So $\mathbb{Q} \leq \mathbb{Q}(u)$ is infinite dimensional.

Theorem

Let $E \leq F$ be a field extension, and let $u \in F$.

1. *If u is algebraic over E, of degree n, then $E \leq E(u)$ is algebraic, and*

   $$E(u) \simeq \frac{E[x]}{p(x)},$$

   where the minimal polynomial $p(x)$

   1. *is irreducible*
   2. *has degree n*
   3. *is the unique (up to association) non-zero polynomial of smallest degree such that $p(u) = 0$*

2. *If u is transcendental over E, then $E \leq E(u)$ is transcendental, and infinite dimensional, and*

   $$E(u) \simeq E(x),$$

   the field of rational functions with coefficients in E.

Proof

- Consider

$$\phi : E[x] \to F$$
$$\phi(f(x)) = f(u)$$

- The image is a subring of F, and is contained in $E(u)$. In fact, it is $E[u]$, the smallest *subring* containing u.
- Let $I = \ker \phi$.
-
  - If $I \neq (0)$, then $I = (p(x)$ for a polynomial, which is (up to association) the unique polynomial of smallest degree in I.
  - Of course $p(u) = 0$; every pol in I has u as a zero, by definition.
  - By the first iso thm, $E[x]/I \simeq E[u] \subseteq E(u) \subseteq F$.
  - So $E[u]$, a subring of a field, is a domain; so I is a prime ideal; so $p(x)$ is irreducible; so I is maximal; so $E[x]/I$ is a field; so $E[u]$ is already a field; so $E[u] = E(u)$.

Proof, cont

- - If $I = (0)$, then ϕ is injective.
  - Then it factors through the splitting field $E(x)$ of $E[x]$. That is, it extends to

$$\hat{\phi} : E(x) \to F$$
$$\hat{\phi}(\frac{f(x)}{g(x)}) = \frac{f(u)}{g(u)}$$

  - It is injective, by general nonsense
  - The image is precisely $E(u)$, the simple extension
  - So $E(x) \simeq E(u)$.

□

This explains "if not identical, then different"; two rational expressions in the transcendental u are equal iff they coincide as rational functions.

Example

Let $\mathbb{Q} \leq \mathbb{C} \ni \sqrt{2} + i = u$. What is $\mathbb{Q}(u)$?
We see that

$$\begin{aligned} u^2 &= 2 - 1 + \sqrt{2}i \\ \sqrt{2}i &= u^2 - 1 \\ -2 &= (u^2 - 1)^2 \\ u^4 - 2u^2 + 3 &= 0 \end{aligned}$$

Since $f(x) = x^4 - 2x^2 + 3 \in \mathbb{Q}[x]$ is irreducible, it is the minimal polynomial of U, and

$$\mathbb{Q}(u) \simeq \frac{\mathbb{Q}[x]}{(x^4 - 2x^2 + 3)}$$

We have that $[\mathbb{Q}(u) : \mathbb{Q}] = 4$.

Definition

Let $E \leq F$, and let $u_1, \ldots, u_r \in F$. We define $E(u_1, \ldots, u_r)$ either as

- The smallest extension of E inside F which contains $u_1, \ldots, u_r$, i.e.,

$$\bigcap_{\substack{E \leq K \leq F \\ u_1, \ldots, u_r \in K}} K,$$

- or as the iterated extension

$$E(u_1)(u_2) \cdots (u_r)$$

Example

Consider $\mathbb{Q}(\sqrt{2})(\sqrt{3})$. We have that $\mathbb{Q}(\sqrt{2})$ has a $\mathbb{Q}$-basis $\{1, \sqrt{2}\}$, and that $\sqrt{3} \not\in \sqrt{3}$. In fact, $x^2 - 3$ is irreducible both over $\mathbb{Q}$ and over $\mathbb{Q}(\sqrt{3})$, so it is the minimal polynomial of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$. The tower theorem, and its proof, then yields that $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ has a $\mathbb{Q}$-basis

$$1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3}.$$

Now consider $u = \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Obviously, $\mathbb{Q} \leq \mathbb{Q}(u) \leq \mathbb{Q}(\sqrt{2}, \sqrt{3})$, where the first inclusion is proper. By the tower theorem again, $[\mathbb{Q}(u) : \mathbb{Q}]$ is a divisor of $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$, so it is either 2 or 4. But $u \not\in \mathbb{Q}(\sqrt{2})$, so it is 4; and $\mathbb{Q}(u) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Theorem

The extension $E \le F$ is finite dimensional iff there are a finite number of elements $u_1, \dots, u_r \in F$, algebraic over E, such that $F = E(u_1, \dots, u_r)$.

Proof.

If $[F : E] = n < \infty$ then there is a basis $u_1, \dots, u_n \in F$. These basis elements are elgebraic over E.

If there are such algebraic elements, then clearly u_j is algebraic over $E(u_1, \dots, u_{j-1})$, and $[E(u_1, \dots, u_{j-1}, u_j) : E(u_1, \dots, u_{j-1})] \le [E(u_j) : E]$, so by the tower theorem,

$$[F : E] = [E(u_1, \dots, u_r) : E] \le [E(u_1) : E] \cdots [E(u_r) : E] < \infty.$$

□

Theorem (Primitive element thm)

Let $E \leq F$ be a finite dimensional extension, and suppose that either $\mathrm{char}(E) = 0$ (that is, $\mathbb{Q} \leq E$) or that E is finite. Then there exists a primitive element $u \in F$ for the extension: $F = E(u)$.

Proof.

The proofs are in Svensson, maybe also in Judson. □

Example

Consider the iterated simple extension

$$\mathbb{Z}_2 \leq E \leq F, \qquad E = \frac{\mathbb{Z}_2[x]}{(x^2+x+1)}, \qquad F = \frac{E[y]}{(y^3+y+1)}$$

Clearly

$$F = \mathbb{Z}_2(\overline{x}, \overline{y}) = \mathrm{span}_{\mathbb{Q}}(1, \overline{x}, \overline{y}, \overline{xy}, \overline{y}^2, \overline{xy}^2).$$

Let's find a primitive element!

Put $v = \overline{x} + \overline{y}$. Then

$$[1, v, v^2, v^3, v^4, v^5]$$

Example

is

$$[1, x+y, y^2+x+1, xy^2+xy, y^2+x+y, xy^2+y^2+x+y]$$

We take the coordinate vectors of these (w.r.t. our prefered basis) and put them in a matrix. Then these 6 powers span F iff they are linearly independent iff the matrix is invertible iff it has determinant 1 in $\mathbb{Z}_2$. The matrix is

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

and it has determinant 1. So $\mathbb{Z}_2(\overline{x}+\overline{y}) = \mathbb{Z}_2(\overline{x},\overline{y}) = F$.

Example

Let $F = \mathbb{Z}_2(t, u)$, rational functions in two variables, and let $E = \mathbb{Z}_2(t^2, u^2)$. Then E is a subfield of F, and $E \leq F$ is an algebraic extension of degree 4. There is, however, no primitiv element for this extension.

Suppose that $a \in F \setminus E$. Then $a^2 \in E$ (because characteristic 2) hence it is a root of $f(x) = x^2 - a^2 \in E[x]$. This must be the minimal polynomial of a, and $E \leq E(a) \leq F$ is a non-trivial intermediate field. Hence a is no primitive element.

Definition

Let $E \leq F$, and let

$$f(x) = \sum_{i=0}^{n} a_i x^i \in E[x]$$

Then $u \in F$ is a zero of $f(x)$ if

$$f(u) = \sum_{i=0}^{n} a_i u^i = 0 \in F$$

It is a simple zero if

$$(x-u) | f(x) \text{ but } (x-u)^2 \not| f(x),$$

and more generally, a zero of multiplicity r if

$$(x-u)^r | f(x) \text{ but } (x-u)^{r+1} \not| f(x).$$

Theorem (Kronecker)

Let $f(x) = \sum_{i=0}^{n} a_i x^i \in E[x]$ be non-constant. Then $f(x)$ has a zero somewhere.

Proof.

Let $f(x) = g(x)h(x) \in E(x)$, with $g(x)$ irreducible. Put

$$F = \frac{E[x]}{(g(x))}.$$

Then $E \leq F$, and $\overline{x} \in F$ is a zero of $f(x)$. □

This might look like some dubious sleight-of-hand, but it is completely on the up-and-up!

Example

The polynomial $f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$ is irreducible, hence has no linear factor, hence no zero (in $\mathbb{Z}_2$). In

$$F = \frac{\mathbb{Z}_2[x]}{(x^2 + x + 1)},$$

the elements are

$$0, 1, \overline{x}, \overline{x} + 1,$$

with the relation

$$\overline{x}^2 = \overline{x} + 1.$$

Now $f(x) = x^2 + x + 1$, viewed as a polynomial with coefficients in F, has two zeroes:

$$f(\overline{x}) = \overline{x}^2 + \overline{x} + 1 = 0$$

$$f(\overline{x} + 1) = (\overline{x} + 1)^2 + (\overline{x} + 1) + 1 = \overline{x}^2 + 1 + \overline{x} + 1 + 1 = 0$$

Definition

Let $E \leq F$. The polynomial

$$f(x) = \sum_{i=0}^{n} a_i x^i \in E[x]$$

is said to split inside the extension F if there are distinct zeroes $u_1, \ldots, u_r \in F$, and multiplicities $b_j \in \mathbb{Z}_+$, such that

$$f(x) = a^n \prod_{j=1}^{r} (x - u_j)^{b_j}$$

Example

The polynomial $f(x) = x^2 + 2 \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$ but splits over $\mathbb{Q}(\sqrt{2}, i)$, since

$$x^2 + 2 = (x - i\sqrt{2})(x + i\sqrt{2}) \in \mathbb{Q}(\sqrt{2}, i)[x].$$

Example

The polynomial $f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$ splits over the "Kronecker extension" we studied earlier, as

$$x^2 + x + 1 = (x + \overline{x})(x + \overline{x} + 1).$$

Definition

The polynomial

$$f(x) = \sum_{i=0}^{n} a_i x^i \in E[x]$$

has F as its *splitting field* if

1. $E \leq F$,
2. $f(x)$ splits in $F[x]$,
3. Write

$$f(x) = a^n \prod_{j=1}^{r} (x - u_j)^{b_j}$$

   Then $F = E(u_1, \ldots, u_r)$

So, we adjoin zeroes of $f(x)$, but nothing unnecessary.

Theorem

The polynomial

$$f(x) = \sum_{i=0}^{n} a_i x^i \in E[x]$$

has a splitting field F, and this splitting field is unique up to a rigid isomorphism:

$$\begin{array}{ccc} F & \xrightarrow{\phi} & L \\ {\scriptstyle i}\uparrow & & \uparrow{\scriptstyle j} \\ E & \xrightarrow{id} & E \end{array}$$

The degree $[F : E] \leq n!$ and if $f(x)$ is irreducible then $[F : E] \geq n$.

Proof.

Read your textbook! □

Example (The most famous splitting field example there is!)

Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. What is its splitting field? Put

$$\alpha = \sqrt[3]{2}$$

$$\beta = \exp\left(\frac{2\pi i}{3}\right) = -\frac{1}{2} + i\frac{\sqrt{2}}{3}$$

which have minimal defining polynomial relations (over Q)

$$\alpha^3 - 2 = 0$$

$$\frac{\beta^3 - 1}{\beta - 1} = \beta^2 + \beta + 1 = 0$$

Example (Cont)

Then, in $\mathbb{Q}(\alpha, \beta)$, $f(x)$ splits as

$$x^3 - 2 = (x - \alpha)(x - \alpha\beta)(x - \alpha\beta^2)$$

So the splitting field is contained in $\mathbb{Q}(\alpha, \beta)$, and of course contains the zeroes

$$\alpha, \ \alpha\beta, \ \alpha\beta^2.$$

But then it also contains $\frac{\alpha\beta}{\alpha} = \beta$, so it is actually equal to $\mathbb{Q}(\alpha, \beta)$. Since $x^3 - 2 \in \mathbb{Q}[x]$ is irreducible, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. We have that

$$(x - \alpha\beta)(x - \alpha\beta^2) = x^2 + x + 1$$

is irreducible over $\mathbb{Q}(\alpha)$, so $[\mathbb{Q}(\alpha)(\beta) : \mathbb{Q}(\alpha)] = 2$; the tower theorem now reveals that $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 3 * 2 = 6$.

Example (Cont)

Note:

- $\alpha \in \mathbb{R}$, so $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$
- α has minimal polynomial $x^3 - 2$ over $\mathbb{Q}$
- This minimal polynomial factors over $\mathbb{Q}(\alpha)$ as

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

  where the latter factor is irreducible
- In particular, we have not found the splitting field after adjoining α to $\mathbb{Q}$.

Example

Let $f(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$. It is irreducible. In $F[y] = \frac{\mathbb{Z}_2[x]}{(x^3+x+1)}[y]$, we have that

$$y^3 + y + 1 = (y + \overline{x}) * (y + \overline{x}^2) * (y + \overline{x}^2 + \overline{x})$$

So, F is the splitting field, since $[F : \mathbb{Z}_2] = 3$.
We found the splitting field after adjoining just one zero!

Example

Let $f(x) = x^4 + 4 \in \mathbb{Q}[x]$. Then

$$f(x) = x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2),$$

By Eisenstein's criteria, these two factors are irreducible. Further analysis reveals that the splitting field has degree two over $\mathbb{Q}$.

Example

Let p be a prime number, and let $f(x) = x^p - 1 \in \mathbb{Q}[x]$. Then

$$f(x) = x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + x1),$$

and the latter factor (call it $g(x)$) can be shown to be irreducible. The zeroes of $g(x)$ are

$$\left\{ \xi^k \middle| 1 \leq k \leq p-1 \right\}, \qquad \xi = \exp(\frac{2\pi i}{p})$$

and the splitting field is $\mathbb{Q}(\xi)$, which has degree $p-1$ over $\mathbb{Q}$.

Example

Let p be a prime number, and let $f(x) = x^p - 2 \in \mathbb{Q}[x]$. Then the splitting field of $f(x)$ is an extension of degree $p(p-1)$.

Prove this on your own as an exercise!

Lemma

Let $E \leq F$ be a field extension. The set of elements of F that are algebraic over E forms a field, which is an algebraic extension over E.

Example

Let $\mathbb{Q} \leq \mathbb{C}$. The set of complex numbers that are algebraic over $\mathbb{Q}$ is called the *field of algebraic numbers*. By definition, any zero of a rational polynomial is an algebraic number. More surprisingly, every zero of a polynomial with algebraic number coefficients — is an algebraic number!

Definition

The field $\overline{K}$ is an *algebraic closure* of K if

1. $K \leq \overline{K}$
2. the extension is algebraic
3. every $f(x) \in K[x]$ splits over $\overline{K}[x]$.

Example

$\overline{Q}$, the field of algebraic numbers, is an algebraic closure of $\mathbb{Q}$.

Definition

The field E is *algebraically closed* if every non-constant $f(x) \in E[x]$ has a zero in E.

Lemma

If E is algebraically closed, and $f(x) \in E[x]$, then $f(x)$ splits in E.

Proof.

Since $f(x)$ has a zero $u \in E$, it has a factor $(x - u) \in E[x]$. Split it off; the remaining factor also has a zero, and so on. □

Theorem (Fundamental theorem of algebra)

The complex field $\mathbb{C}$ is algebraically closed.

Lemma

Let $\overline{K}$ be an algebraic closure of K. Then $\overline{K}$ is algebraically closed (so equal to its closure).

Proof.

1. Take a polynomial $f(x) \in \overline{K}$, and pick a zero u (somewhere).
2. Then $\overline{K} \leq \overline{K}(u)$ is algebraic.
3. Furthermore $K \leq \overline{K}$ is algebraic.
4. This means that $K \leq \overline{K}(u)$ is algebraic.
5. In particular, u is algebraic over K.
6. But then it belongs to $\overline{K}$.
7. Hence, all zeroes of polynomials in $\overline{K}[x]$ remain in $\overline{K}$.
8. So this field is algebraically closed.

□

Theorem

Let E be a field. Then there exists a unique (up to rigid isomorphism) algebraic closure $\overline{E}$, i.e.

1. $E \leq \overline{E}$, *and this extension is algebraic*
2. *Any polynomial with coefficients in E have a zero in $\overline{E}$,*
3. *Any polynomial with coefficients in $\overline{E}$ have a zero in $\overline{E}$,*

Proof.

Needs set theory yoga. □

Example

$\mathbb{Q} \le \overline{Q} \le \mathbb{C} \le \mathbb{C}(x)$. The field of algebraic numbers is

1. the algebraic closure of $\mathbb{Q}$,
2. algebraically closed,
3. the set of complex numbers that are algebraic over $\mathbb{Q}$.

The complex field $\mathbb{C}$ algebraically closed, and its own algebraic closure. It is still properly contained in the field of rational functions with complex coefficients — this latter field is *not* algebraically closed! I belive he algebraic closure is the field of *Puisseux series*.

Recall that a complex number α is algebraic over $\mathbb{Q}$ if it is the zero of a non-trivial polynomial with rational coefficients, i.e., if

$$c_n\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0, \qquad c_j \in \mathbb{Q},\ c_n \neq 0,\ n \geq 1$$

Definition

The complex number α is an *algebraic integer* if it is the zero of a monic polynomial with integer coefficients, i.e. if

$$c_n\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0, \qquad c_j \in \mathbb{Z},\ c_n = 1,\ n \geq 1$$

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Example

Let $q = \sqrt{1/2}$. Then $q^2 = 1/2$, so q has minimal polynomial $x^2 - 1/2$. Let $I \subset \mathbb{Q}[x]$ consist of those polynomials that have q as a zero. Then $I = (x^2 - 1/2)$. It contains monic polynomials and polynomials with integer coefficients (such as $2x^2 - 1$) but no monic polynomial with integer coefficients. So the algebraic number q is not an algebraic integer. Hovever, $2q$ has minimal polynomial $x^2 - 2$, so it is an algebraic integer.

Theorem

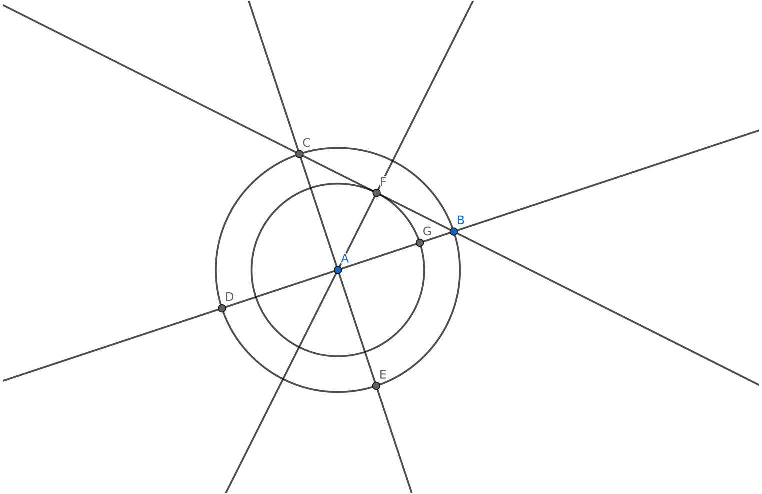
If $\alpha \in \mathbb{C}$ is an algebraic number, then $n\alpha$ is an algebraic integer for some positive integer n.

Construction with straightedge and compass

- Can't trisect an angle!
- Can't double a cube!
- Can't square a circe!

At least not a general angle et cetera, and using only an (unmarked) straightedge (linjal) and a compass (passare), and finitely many operations (no limits).

- You are given a plane, and in the plane, two points.
- The distance between the points is, by definition, 1.
- You can construct new lines and new circles by drawing the line between to constructed points, and drawing the circle with midpoint a constructed points, and another constructed point on its periphery.
- Intersection points between lines and lines, between lines and circle, between circles and circles, are also constructed (or constructible) points.
- Keep going indefinitely, get a subset of constructible points in the plane.
- The x and y coordinates of constructible points form a subset of $\mathbb{R}$, the constructible real numbers.

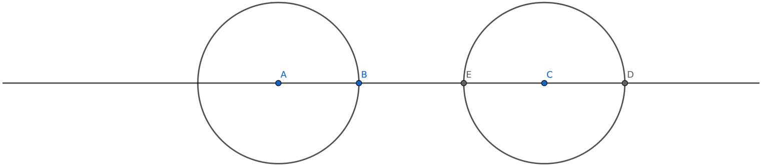


G has x-coordinate $1/\sqrt{2}$, which is hence constructible. (A general point on the lines/circles is not constructed).

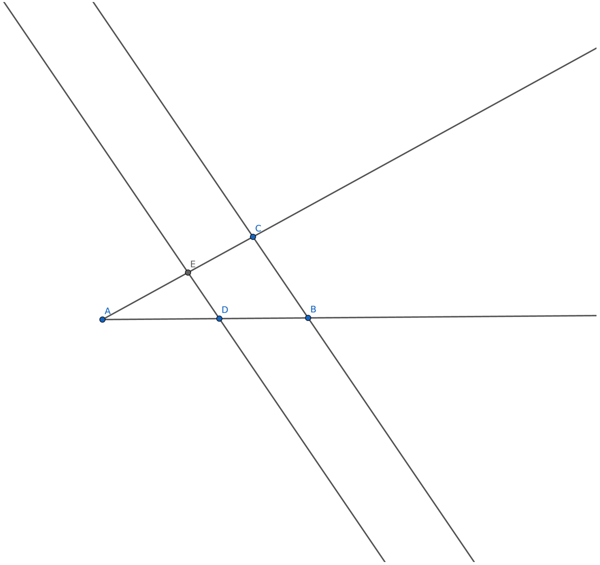
Theorem

1. *The set of constructible numbers form a subfield of* $K \leq \mathbb{R}$.
2. $[K : \mathbb{Q}] = \infty$
3. *For* $u \in K$, $[\mathbb{Q}(u) : \mathbb{Q}] = 2^n$, *for some* n *(which depends on* u*).*
4. *In fact,* u *is constructible iff there is some finite chain of simple quadratic radical extensions*

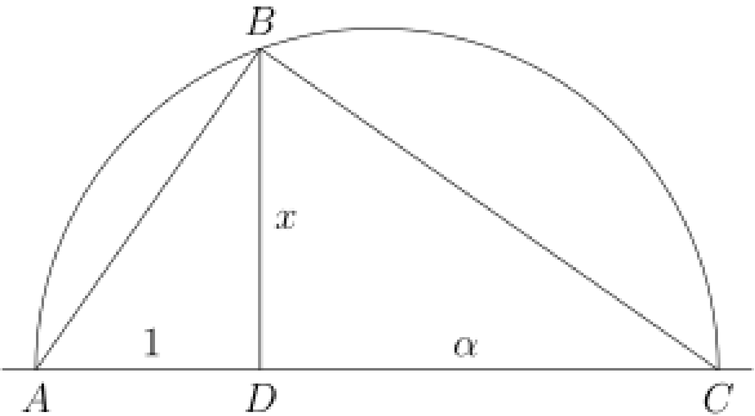
$$\mathbb{Q} \leq \mathbb{Q}(\sqrt{\alpha_1}) \leq \mathbb{Q}(\sqrt{\alpha_2}) \leq \cdots \leq \mathbb{Q}(\sqrt{\alpha_n}) = \mathbb{Q}(u)$$



$AB = \alpha$, $AC = \beta$, $\alpha + \beta$ and $\alpha - \beta$ constructed.



$AB/AD = AC/AE$, so take $AC = 1$, $AD = x$, $AB = y$,get $AE = x/y$.



Square root of α.

Coefficients in K.

- Line L: $Ax + By + C = 0$
- Circle S_1: $(x - d_1)^2 + (y - d_2)^2 - r_1 = 0$
- Circle S_2: $(x - d_3)^2 + (y - d_4)^2 - r_2 = 0$

Intersection $L \cap S_1$: $y = (-A/B)x - C/B$ so

$$\begin{aligned} 0 &= (x - d_1)^2 + ((-A/B)x - C/B) - d_2)^2 - r_1 \\ &= ux^2 + vx + w, \qquad u, v, w \in K \\ &= u(x^2 + v/ux + w/u) \\ &= u\left((x - v/(2u))^2 - v^2/(4u^2) + w/u\right) \end{aligned}$$

with zeroes in $K(\sqrt{v^2/(4u^2) - w/u})$.

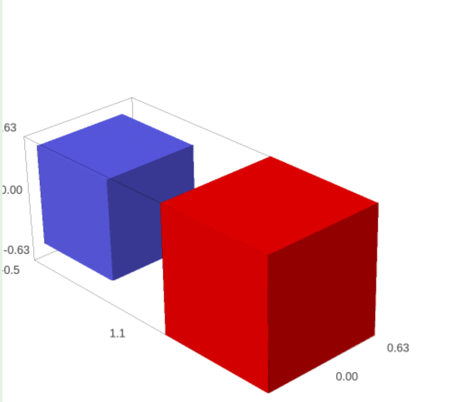
Example

- Any rational number is constructible
- $$\sqrt{3/4 + \sqrt{7/3}}$$
  is constructible
- $\cos(\pi/3)$ is constructible
- $\alpha = \cos(\pi/9)$ is not constructible, since
  $$1/2 = \cos(\pi/3) = \cos(3 * \pi/9) = 4\cos^3(\pi/9) - 3\cos(\pi/9)$$
  and hence α is a root of
  $$4x^3 - 3x - 1/2 = 0$$
  where the LHS is a irreducible polynomial; hence $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, not a power of two.

Doubling the cube

Example

The number $2^{1/3}$ is algebraic of degree 3, hence not constructible. So one can not construct, with straightedge and compass, the side length of a cube of volume 2.



Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Example

It is impossible to "square the circle", i.e. construct a square with the same area as a unit circle, since π is transcendental.