4-16-25 (WEEK 9)

Shun/翔海 (@shun4midx)

# ALGEBRAIC EXTENSION

## DEFINITION

$L/K$ is said to be algebraic if $\forall \alpha \in L$, $\alpha$ is alg over $K$.

## PROPOSITION 1

(When we wanna prove "alg", we always try to prove finiteness for $[K(\alpha):K]$.)

$[L:K] < \infty \Leftrightarrow L = K(\alpha_1, \dots, \alpha_n)$, where $\alpha_i$ is alg over $K$ $\forall i$ (In this case, $L/K$ is algebraic)

Proof

"$\Rightarrow$": Let $[L:K]=n$ and $\{\alpha_1, \dots, \alpha_n\}$ be a basis for $L$ over $K$

$\because L = K\alpha_1 + \dots + K\alpha_n = K(\alpha_1, \dots, \alpha_n) \subseteq L$

$\therefore L = K(\alpha_1, \dots, \alpha_n)$

Now, $\forall i$, $[K(\alpha_i):K] \le [L:K] < \infty$ $\therefore \alpha_i$ is alg over $K$

"$\Leftarrow$": $[L:K] = [K(\alpha_1, \dots, \alpha_n) : K(\alpha_1, \dots, \alpha_{n-1})] \cdots [K(\alpha_1):K] < \infty$ (algebraic over) □

Moreover, $\alpha \in K(\alpha_1, \dots, \alpha_n) \Rightarrow [K(\alpha):K] \le [L:K] < \infty \Rightarrow \alpha$ is alg over $K$

## COROLLARY

Given $L/K$ and $S$ as a subset of $L$, if $\forall \alpha \in S$, $\alpha$ is alg over $K$, then $K(S)/K$ is alg

Proof

(When we pinpoint an element, etc these is finiteness)

$\forall \alpha \in K(S)$, $\exists \alpha_1, \dots, \alpha_n \in S$, s.t. $\alpha \in K(\alpha_1, \dots, \alpha_n)$ $\therefore \alpha$ is alg over $K$. □

## PROPOSITION 2

If $M/L$ and $L/K$ are alg, then $M/K$ is alg

Proof

$\forall \alpha \in M$, we know $\alpha$ is alg over $L$, say $\alpha^n + a_1\alpha^{n-1} + \dots + a_n = 0$, $a_i \in L$. This means that $\alpha$ is alg over $K(a_1, \dots, a_n)$

Now, notice $[K(a_1, \dots, a_n, \alpha) : K] = [K(a_1, \dots, a_n, \alpha) : K(a_1, \dots, a_n)][K(a_1, \dots, a_n) : K] < \infty$ ($\alpha$: $\infty$, $a_i$: $\infty$)

## DEFINITION

- $L$ is algebraically closed if each nonconstant $f(x) \in L[x]$ has a root in $L$ (not just "a root in $L$")
- $\bar{K}$ is an algebraic closure of $K$ if $\bar{K}/K$ is alg and $\forall f(x) \in K(x)$, it splits completely over $L$

## FACT 1

$K$ is algebraically closed $\Leftrightarrow K = \bar{K}$

Proof

"$\Rightarrow$": Claim: $\forall f(x) \in K(x)$, $f(x)$ splits over $K$

Proof (intuition: recursively divide, we still have a root in $K$)

By induction on $n = \deg f$,

- $n=1$: $f(x) = ax+b = a(x+\frac{b}{a})$
- $n>1$: Let $\alpha \in K$ be a root of $f(x)$. We have $f(x) = (x-\alpha)f_1(x)$ where $f_1(x) \in K(\alpha)[x] = K[x]$ and $\deg f_1 < n$

$\therefore f_1(x) = \lambda(x-\alpha_1)\cdots(x-\alpha_{n-1})$, $\alpha_i \in K$ ✓

"$\Leftarrow$": $\forall f \in K[x]$, $f(x)$ splits over $\bar{K} = K$, i.e. $f(x) = \lambda(x-\alpha_1)\cdots(x-\alpha_n)$ for $\alpha_i \in K$ $\therefore f(\alpha_i) = 0$

## FACT 2

If $\bar{K}$ is an alg closure of $K$, then $\bar{K}$ is alg closed

Proof

Let $f(x) \in \bar{K}[x]$ and $\alpha$ be a root of $f(x)$. Then, $\bar{K}(\alpha)/\bar{K}$ is alg

By def, $\bar{K}/K$ is alg, so $\bar{K}(\alpha)/K$ is alg $\therefore \alpha$ is alg over $K$, i.e. $\alpha \in \bar{K}$ □

Shun/翔海 (@shun4midx)

**FACT 3**

Given $L/K$, if $L$ is algebraically closed, then $L_\alpha = \{\alpha \in L \mid \alpha \text{ is alg over } K\} = \bar{K}$

Proof

$\forall f(x) \in K(x) \subseteq L[x]$, $f(x) = \lambda(x-\alpha_1)\dots(x-\alpha_n)$ for some $\alpha_i \in L$. Hence, $\alpha_i \in L_\alpha \ \forall i$, i.e. $f(x)$ splits over $L_\alpha$

**THEOREM**

If $K$ is a field, then $\bar{K}$ exists.

Proof (variable, not element)

Let $S = \{x_f \mid f \in K[x], \deg f \geq 1\}$

Consider the poly ring $K[S]$ and $I = \langle f(x_f) : \deg f \geq 1 \rangle \subset K[S]$

Claim: $I \neq K[S]$ ($\Rightarrow \exists M \in \mathrm{Max}\, K[S]$, s.t. $M \supseteq I$. Let $F_1 = K[S]/M$ which is a field and $K \hookrightarrow F_1$, then $f(\bar{x}_f) = 0$) (element, no longer variable)

Proof

Assume not, i.e. $I = K[S]$, say $1 = g_1 f_1(x_{f_1}) + \dots + g_n f_n(x_{f_n})$, $g_i \in K[S]$

Write $x_i := x_{f_i}$ and assume $g_i \in K(x_1, \dots, x_m]$, $m \geq n$

Also, $\exists \alpha_i \in \Omega \supseteq K$ (just any root for $f_i$), s.t. $f_i(\alpha_i) = 0$, $\alpha_j = 0 \ \forall j > n$. Then, $1 = g(\alpha_1, \dots, \alpha_m) f_1(\alpha_1) + \dots + g(\alpha_1, \dots, \alpha_n) f_n(\alpha_n) = 0$ ↯

By induction, $\exists F_1 \subseteq F_2 \subseteq F_3 \subseteq \dots$ s.t. $\forall f \in F_n[x]$, $\exists$ a root in $F_{n+1}$

Now, let $F = \bigcup_{i \geq 1} F_i$ which is a field and is alg closed by construction.

Finally, we take $\bar{K} = \{\alpha \in F \mid \alpha \text{ alg over } K\}$ □

# GEOMETRIC CONSTRUCTION

**DEFINITION** ($z_1 = 0, z_2 = 1$)

Given $\{z_1, \dots, z_n\} \in \mathbb{C}$, $C(z_1, \dots, z_n) = \{z \in \mathbb{C} \mid z \text{ is constructable by rule and compass from } z_1, \dots, z_n\}$

($S_1 = \{z_1, \dots, z_n\} \rightsquigarrow S_2 \rightsquigarrow S_3 \rightsquigarrow \dots$, $C(z_1, \dots, z_n) = \bigcup_{i \geq 1} S_i$)

Notice, $S_{i-1}$ lines: Any straight line between any two points in $S_{i-1}$

$S_{i-1}$ circles: Any circle with a center in $S_{i-1}$ and another point in $S_{i-1}$ as its radius away

Now, we construct $S_i$ with the following within $S_{i-1}$

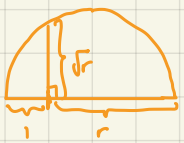
↪ I: Any intersection between two lines

↪ II: Any intersection between a line and a circle

↪ III: Any intersection between two circles

**FACT 4**

$C(S_1, \dots, S_n)$ is a subfield of $\mathbb{C}$ (Proof idea: $z = re^{i\theta}$, multiplication done with similar triangles)




**FACT 5**

$z \in C(S_1, \dots, S_n) \Rightarrow \bar{z}, z^{\frac{1}{2}} \in C(S_1, \dots, S_n)$ (Proof idea for $\sqrt{z}$: $\sqrt{z} = \sqrt{r}e^{i\frac{\theta}{2}}$. Angle bisection $\Rightarrow \frac{\theta}{2}$ is OK. $\sqrt{r}$ can be done with semicircle)

**PROPOSITION 3**

$C(z_1, \dots, z_n)$ is the smallest subfield of $\mathbb{C}$ containing $z_1, \dots, z_n$ and closed under conjugation and square roots

Proof

Let $C'$ be any subfield of $\mathbb{C}$. Hope "$C' \supseteq C(z_1, \dots, z_n)$"

Observe: • $-1 \in C' \Rightarrow \sqrt{-1} = i \in C'$

• $x + iy \in C'$, $x, y \in \mathbb{R} \Rightarrow x, y \in C'$, since $x + iy \in C'$, $\overline{x+iy} = x - iy \in C'$

Shun/翔海 (@shun4midx)

Also, any line through distinct points in $C'$ has $ax+by+c=0$, $a,b,c\in C'$
any circle constructed from $C'$ has $x^2+y^2+dx+ey+f=0$, $d,e,f\in C'$ or $(x-a)^2+(y-b)^2=c$, $a,b,c\in C'$

from (I), (II), (III), we know any intersection point still lies in $C'$. Hence, $C'\supseteq C(z_1,\dots,z_n)$. □

## THEOREM 2

Let $z_1=0$, $z_2=1$, $\dots$, $z_n\in\mathbb{C}$ and $F=\mathbb{Q}(z_1,\dots,z_n,\bar{z}_1,\dots,\bar{z}_n)$

Then, $C(z_1,\dots,z_n)=\{z\in\mathbb{C}\mid \exists u_1,\dots,u_r \text{ with } u_i^2\in F,\ u_i\in F(u_1,\dots,u_{i-1}) \text{ s.t. } z\in F(u_1,\dots,u_r)\}$ (say RHS $=:C''$)

Proof

"$\supseteq$": By fact 5, $F\subseteq C(z_1,\dots,z_n)\Rightarrow u_1\in C(z_1,\dots,z_n)\Rightarrow u_2\in C(z_1,\dots,z_n,u_1)=C(z_1,\dots,z_n)$

Continue this logic, we get $F(u_1,\dots,u_r)\subseteq C(z_1,\dots,z_r)$

"$\subseteq$":
- $C''$ is a subfield: $z\in F(u_1,\dots,u_r)$, $z'\in F(u_1',\dots,u_s')\in C''\Rightarrow z\pm z'$, $zz'$, $z^{-1}$, $(z')^{-1}\in F(u_1,\dots,u_r,u_1',\dots,u_s')$ ✓
- For $z\in C''$, say $z\in F(u_1,\dots,u_r)$, then $\sqrt{z}\in F(u_1,\dots,u_r,\sqrt{z})$ $\therefore\sqrt{z}\in C''$
- For $\bar{z}\in C''$, say $\bar{z}\in F(u_1,\dots,u_r)$, then $\bar{z}\in\overline{F(u_1,\dots,u_r)}=F(\bar{u}_1,\dots,\bar{u}_r)$ $\therefore\bar{z}\in C''$

$\therefore$ The result follows from proposition 3. □

## COROLLARY

If $z\in C(z_1,\dots,z_n)$, then $[F(z):F]=2^m$ for some $m\in\mathbb{N}$

Proof

Let $z\in F(u_1,\dots,u_r)$. Observe that if $u_i\in F(u_1,\dots,u_{i-1})$, then $[F(u_1,\dots,u_i):F(u_1,\dots,u_{i-1})]=1$

if $u_i\notin F(u_1,\dots,u_{i-1})$, then $[F(u_1,\dots,u_i):F(u_1,\dots,u_{i-1})]=2$

$\therefore$ Continuing this process, we get $[F(u_1,\dots,u_r):F]=2^s$ and $[F(z):F]\mid 2^s\Rightarrow[F(z):F]=2^m$ □

## REMARK (3 big questions)

1. If a unit cube has volume 1, ∄ cube s.t. volume=2?
   ↳ $z=\sqrt[3]{2}\rightsquigarrow x^3-2$ $\therefore[\mathbb{Q}(z):\mathbb{Q}]=3$ ✗ (not power of 2)
2. ∄ square of area $\pi$?
   ↳ $z=\sqrt{\pi}\rightsquigarrow x^2-\pi$ $\therefore[\mathbb{Q}(\pi):\mathbb{Q}]=\infty$ ✗
3. $z=\cos 20^\circ$ is drawable? $\rightsquigarrow\frac{1}{2}=4\cos^3 20^\circ-3\cos 20^\circ\rightsquigarrow 8x^3-6x-1\rightsquigarrow$ deg=3 ✗

Now, about construction of $p$-gons, $p$: a prime, it is equivalent to drawing $z=\cos\frac{2\pi}{p}+i\sin\frac{2\pi}{p}$, $z^p=1\Rightarrow z^{p-1}+z^{p-2}+\dots+1=0$

For this to be drawable, we need $[\mathbb{Q}(z):\mathbb{Q}]=p-1=2^m$, so we only can do so for $p=2^m+1$, $m=2^t$ (but is it for all $p=2^{2^t}+1$?)