MAT401 March 12th 2008

Goal: 1 If $a,b \in E/F$ are algorithm, then so are $a+b$, $a-b$, ab, a/b

2. If $a_i \in E/F$ are alg, and $b \in E$ satisfies $\sum a_i b^i = 0$ then b is algebraic

Today:
1. Algebraic numbers
2. Geometric Constructions
3. Odds & ends from 'chapter 21'.

key pt from last class, If $a \in E/F$ is a root of an irreducible $p \in F[x]$, then $a \mapsto [x]$
$[x] \mapsto a$

$F(a) \tilde{=} F[x]/\langle p \rangle =$ therefore, every element of $F(a)$. can we written uniquely as $c_0 a^0 + c_1 a^1 + \cdots + c_{n-1} a^{n-1}$ $n = \deg p$. $c_i \in F$.

Def: An element $a \in E/F$ is "algebraic" over F if it is the root of some polynomial with coeffs in F.

Def: If E/F say E/F is finite if E is a finite dim vector space over F, $[E:F] = \dim_F E$.

"The degree of E/F"

Thm 1: $a \in E/F$. then a is alg over F iff $[F(a):F] < \infty$ $F(a)/F$ is finite extension.

Proof: $\Rightarrow$: If a is alg, then a is the root of some polynomial $f \in F[x]$, so also the root of some irreducible $p \in F[x]$. by key fact, $n = \deg p$

$E = \{c_0 a^0 + c_1 a^1 + \dots + c_{n-1} a^{n-1} \cdot c_i \in F\}$

$\Rightarrow$ So the collection $\{a^0, a^1, a^2, \dots a^{n-1}\}$ is a basis of $F(a)/F$.

$\Leftarrow$ assume $F(a)/F$ is finite, set $n = [F(a):F]$.

Consider $a^0 a^1 \dots a^{n-1}, a^n$

these are $n+1$ vectors in the n-dim v.s. $F(a)$, so they are lin. dep. i.e.

$\exists c_i$ $i = 0, \dots, n$, $c_i \in F$. not all $= 0$

$\sum c_i a^i = 0$ so a is a root of $\sum c_i x^i$.

Thm 2: $K/E/F$ then $[K:F] = [K:E][E:F]$ (true even if one of these is ∞)

Claim: If $a, b \in E/F$ are alg, so are $a+b$, $a-b$, $a \cdot b$, a/b

Proof: $a+b$, $a \cdot b$, $a-b$, a/b, $\frac{a^3 - b^2}{b+a} \in F(a,b)$

$\Rightarrow F(a+b) \subset F(a,b)$ If $[F(a,b):F]$ is finite, then $[F(a+b):F] < \infty$,

Thm 1: $a \in E/F$ then a is alg over F iff $[F(a):F] < \infty$ $F(a)/F$ is finite extension

So $a+b$ is alg. likewise ab, $a-b$.

$F(a,b)/F(a)/F$ then $F(a)/F$ is finite as a is alg over F.

and $F(a,b)/F(a)$.

$F(a)[b)/F(a)$ is finite as b is algebraic over F hence also over $F(a)$.

Claim 2. If $a_i \in E/F$ are alg & b satisfies $\sum a_i b^i = 0$, then b is alg.

Proof: Consider the tower.

$F(a_0, a_i, b)$ / Finite $F(a_0, a_n)$ / Finite

$F(a_0 \ldots a_n, b) / F \Leftarrow F(a_0, a_1) = F(a_0)(a_1)$

is finite, so b is algebraic

/ finite

$F(a_0)$

/ finite

F

Thm 2: $K/E/F$ Then $[K:F] = [K:E][E:F]$ (true even if one of these is ∞)

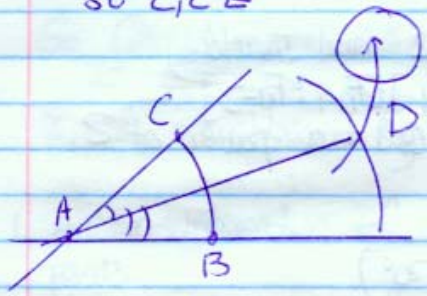
Proof of Thm 2: let (x_i) be a basis of K/E. $(x_i \in K)$. Let (y_j) be a basis of E/F.

Claim: $\{x_i y_j\}$ is a basis of K/F. Indeed, let $z \in K$ be any element. Then

$$z = \sum c_i x_i = \sum \left(\sum b_{ij} y_j\right) x_i = \sum_{ij} b_{ij} x_i y_j .$$

(x_i) spans K/E so $c_i \in E$

with $c_i = \sum b_{ij} y_j$ with $b_{ij} \in F$

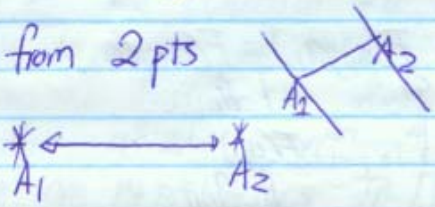


classical Problem

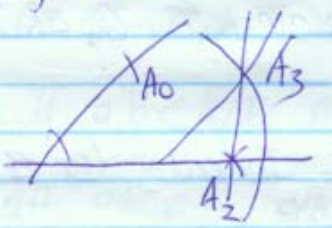
Can you trisect "divide by 3" an angle using a ruler & a compass

Ans: No, cannot given trisect $60°$.

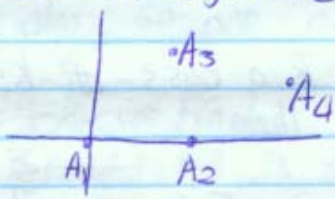
Start from 2 pts



At each step, draw lines by connecting two previously named points, or draw circles of radius = distance between two previously named points & a previously named centre; pick an intersection point and in it A_3, A_4 ...



choose a system of coordinates
s.t $A_1=(0,0)$ $A_2=(1,0)$



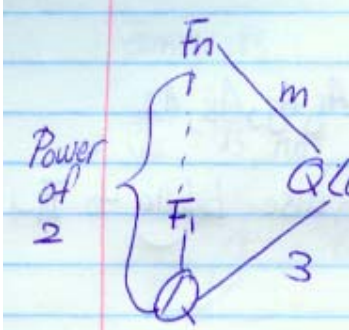
let $F_0=\mathbb{Q}$
let $F_n=F_0(x_1 \ldots x_n, y_1 \ldots y_n)$
$A_k=(x_k, y_k)$.

claim $[F_n : F_{n-1}]$ is 1 or 2 and therefore,
$[F_n, \mathbb{Q}] = [F_n : F_{n-1}][F_{n-1} : F_{n-2}]$
$\cdot [F_1 : F_0 = \mathbb{Q}]$ = a power of 2.

$\cos 20°$

$(\cos 20°, \sin 20°)$
$\cos 20° \in F_n$
for some n.

but
$[\mathbb{Q}[\cos 20°] : \mathbb{Q}] = 3$.



$3 \cdot m =$ a power of $2 \Rightarrow x =$.

$(\cos x + i\sin x)^3 = (e^{ix})^3 = e^{3ix} = \cos 3x + i\sin 3x$
Take real parts.

$\cos^3\alpha - 3\cos\alpha(1-\cos^2\alpha) = \cos^3\alpha - 3\cos\alpha\sin^2\alpha = \cos 3\alpha$
$(1-\cos^2\alpha)$

$\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$
take $\alpha = 20°$
$\frac{1}{2} = \underbrace{4\cos^3 20°}_{a} - 3\cos 20°$

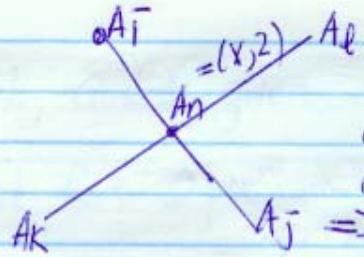
$\frac{1}{2} = 4a^3 - 3a \Rightarrow 8a^3 - 6a - 1 = 0$
so a is a root of $8x^3 - 6x - 1 = m/n$
which is irreducible over $\mathbb{Q}$.

So $\mathbb{Q}(a) = \mathbb{Q}[x]/\langle p \rangle$ so $[\mathbb{Q}(a) : \mathbb{Q}] = 3$

F_n/F_{n-1} is obtained by adding the coordinates of A_n

1. A_n an intersection of two lines defined by existing points.
2. A_n an intersection of a line & a circle.
3. A_n an intersection of 2 circles.

Case I.



$i,j,k,\ell < n$

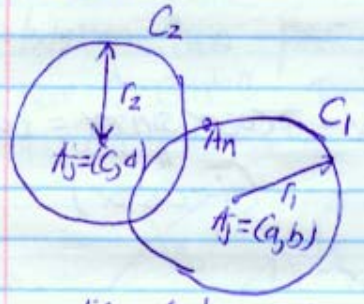
coordinates of A_i, A_j, A_k, A_ℓ are in F_{n-1}

$A_j \Rightarrow$ coords of A_n also belong to F_{n-1}

$\Rightarrow F_n = F_{n-1}$

$[F_n : F_{n-1}] = 1$

Case III



$r_1 = |A_k - A_\ell|$ where

$r_2 = |A_p - A_x|$ $i,j,k,\ell,p,q < n$.

$C_1: (x-a)^2 + (y-b)^2 = r_1^2 = (x_k - x_\ell)^2 + (y_k - y_\ell)^2$

$C_2: (x-c)^2 + (y-d)^2 = r_2^2 = (x_p - x_q)^2 + (y_p - y_q)^2$

1 in eqn relating x & y.

$y = \alpha x + \beta$. where α & $\beta \in F_{n-1}$ Substitute in C_1 so x satisfies.

a quadratic eqn with coefficients $\in F_{n-1}$ so

$[F_n : F_{n-1}] = \{1, 2$

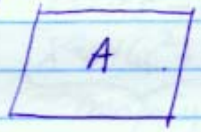
comments

1. $\sqrt[3]{2}$ is not constructible. $r = x^3 - 2 = 0$

$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$

"Cannot double the volume of a cube".

2. π is not algebraic so "cannot square a circle".



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

"E"

$3 \geq ?$ $\quad E = \mathbb{Q}(\sqrt[4]{3}, \sqrt[3]{4}) = \mathbb{Q}(\sqrt[4]{3})(\sqrt[3]{4})$

$? \leq 4$

$\mathbb{Q}(\sqrt[4]{3})$ $\qquad$ $\mathbb{Q}(\sqrt[3]{4})$

$x^4 - 3 = 0$ irred $\qquad$ $\sqrt[3]{4}$ is a root of $x^3 - 4 = 0$

$4 \quad 3$

$\mathbb{Q}$

$x^3 - 4$ irred over $\mathbb{Q}(\sqrt[4]{3})$?

$[E : \mathbb{Q}] \leq 12$

$\| \; d$

$3 \mid d, \; 4 \mid d \Rightarrow d = 12$.

Example 2:

$[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}]$

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

≤ 2 $\qquad$ ≤ 2

$\mathbb{Q}[\sqrt{3}]$ $\qquad$ $\mathbb{Q}[\sqrt{5}]$

$2 \quad 2$

$\mathbb{Q}$

$d = [E : \mathbb{Q}] \leq 4$

$2 \mid d, \; 2 \mid d$

$d = 2, 4, 2$.

claim $\sqrt{5} \notin \mathbb{Q}(\sqrt{3}) \Rightarrow [\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{3})] > 1$

$\Rightarrow = 2$

$\{a + b\sqrt{3} : a, b \in \mathbb{Q}\} \Rightarrow d = 4$

$\sqrt{5} \neq a + b\sqrt{3}$ for $a, b \in \mathbb{Q}$

Def: Suppose $a \in E/F$ is alg, a minimal polynomial p for a is an irred $p \in F[x]$ s.t.

1. $P(a) = 0$
2. P is "monic"
   $P = 1x^n +$ lower powers.

Claim: In this situation, such p exists and is unique.

Proof: Existence. a alg $\Rightarrow \exists\ f \in F[x]$ $f(a) = 0$
$\Rightarrow$ take an
irreducible factor s.t. $P(a) = 0$
$\Rightarrow$ normalize.

Given a, consider

$A = \{f : f(a) = 0\}$ is an ideal in $F[x]$

$p \in A$ & irred $\Leftrightarrow$ P is of minimal degree
but if $P_1(a) = 0$, $P_2(a) = 0$ & both are monic
and of minimal degrees, then $\deg P_1 = \deg P_2$.
so $P_1 - P_2 =$ lower degree, $= 0$.
so $P_1 = P_2$

So prime $p = \text{min poly}(a)$.

1. It is of minimial deg among f s.t $f(a)=0$
2. If $f(a)=0$ then $\text{minpoly}(a) \mid f$.
3. $[F(a):F] = \deg \text{minpoly}(a)$

Example: Determine minpoly of $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}+\sqrt{3}$.

1. x^2-2
2. x^2-3

$x = \sqrt{3}+\sqrt{5}$

$x^2 = 3+5+2\sqrt{15} = 9+2\sqrt{15}$

$x^2-8 = 2\sqrt{15}$

$x^4-16x^2+64 = 60$

$x^4-16x^2+4 = 0$

x^4-16x^2+4 minpoly irred? Yes by showing irreducibility.

$Q(\sqrt{3}+\sqrt{5}) = Q(\sqrt{3},\sqrt{5})$. so $[Q(\sqrt{3}+\sqrt{5}):Q] = [Q(\sqrt{3},\sqrt{5}):Q]$

$= 4$.

so $\deg \text{minpoly}(\sqrt{3}+\sqrt{5}) = 4$.