Lecture 22

<u>defn.</u> Let K_1, K_2 be subfields of K.

The composite field of K_1 and K_2 is K_1K_2 = the smallest subfield containing $K_1 \cup K_2$.

eg. $K_1 = \mathbb{Q}(\sqrt{2})$, $K_2 = \mathbb{Q}(\sqrt[3]{2})$. $K_1K_2 = \mathbb{Q}(\sqrt[6]{2})$

- K_1K_2 must contain $\sqrt{2}$ and $\sqrt[3]{2}$, and therefore also $2^{1/2}/2^{1/3} = 2^{1/6}$.
- $\sqrt{2}, \sqrt[3]{2} \in \sqrt[6]{2}$.

<u>prop.</u>

$$\begin{tikzcd}[column sep=small]
& K \arrow[d, dash] & \\
& K_1K_2 \arrow[dl, dash, "\le d_2"'] \arrow[dr, dash, "\le d_1"] & \\
K_1 \arrow[dr, dash, "d_1"'] & & K_2 \arrow[dl, dash, "d_2"] \\
& F &
\end{tikzcd}$$

ie. $[K_1K_2 : F] \le [K_1 : F][K_2 : F]$

equality iff an F basis for one K_i/F remains linearly indep over the other K_j.

Pf. clear; use VS basis.

<u>Cor.</u> Suppose $\gcd(d_1, d_2) = 1$. Then $[K_1K_2 : F] = d_1 d_2$.

Pf. the degree $[K_1K_2 : F]$ must be a multiple of both d_1 and d_2.

defn. Let $f(x) \in F[x]$. An extension K of F is a splitting field of $f(x)$ if $f(x)$ factors completely into linear factors (ie splits completely) in $K[x]$ and doesn't factor over any proper subfield of K.

We will focus on concrete examples, ie various number fields. But note that you can build abstract splitting fields:

thm. For any field $F[x]$, if $f(x) \in F[x]$, then there exists a splitting field K for $f(x)$.

pf. Recall we were able to construct an extension containing a root of $f(x)$. Factor out the new linear factor and induct.

Fact Any two splitting fields for $f(x) \in F[x]$ over F are isomorphic.

"pf" inductively build an isom:

$$\begin{tikzcd}[column sep=small] F(\alpha) \arrow[rr, phantom, "\cong"] & & F(\varphi(\alpha)) \\ & F \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$

We will not prove this carefully but rather focus on examples / intuition for structure of field extensions.

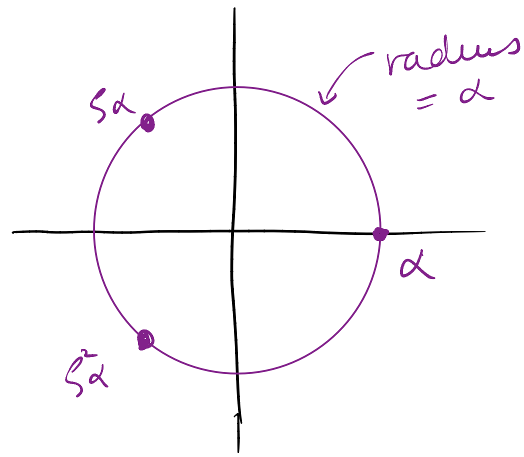
eg. The splitting field of x^3-2?

Let $f(x)=x^3-2$; let $\alpha=\sqrt[3]{2}$.

- $f(x)$ is Eisenstein at $p=2$, so $[\mathbb{Q}(\alpha):\mathbb{Q}]=3$.
- But $f(x)$ does not split in $\mathbb{Q}(\alpha)$! Use our knowledge of complex #s:

Let $\zeta=\zeta_3$ = a primitive 3^{rd} root of unity

↪ familiar?



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

(Clearly $\sqrt{-3}\notin\mathbb{Q}(\alpha)\subset\mathbb{R}$)

Since ζ is a root of x^2+3, $[\mathbb{Q}(\zeta):\mathbb{Q}]=2$.

- Since $\gcd(2,3)=1$, we know $[\mathbb{Q}(\alpha,\zeta):\mathbb{Q}]=6$.

↑ splitting field for $f(x)$

In the "worst case", we keep adding new roots and factoring out linear factors but the remaining polyn is still irreducible.

Therefore

Prop. A splitting field of a polyn of deg n over F is of degree at most $n!$ over F.

eg. Cyclotomic Fields : Splitting field of $x^n - 1$

① The roots of $x^n - 1$ are the n^{th} roots of unity:

Let $\zeta_n = e^{2\pi i/n}$. Roots: $\{1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}\}$.

② A generator of this cyclic group of n^{th} roots of unity is called a primitive n^{th} root of unity.

Fact There are $\varphi(n)$ primitive n^{th} roots

← Euler totient function.

$$\varphi(n) = \#\{m \leq n \mid \gcd(m,n) = 1\}.$$

③ $\Phi_n(x)$ = the minimal polynomial of ζ_n over $\mathbb{Q}$ ($\mathbb{Z}$)

eg. $n=3$: $x^3 - 1 = (x-1)\underbrace{(x^2+x+1)}_{\text{irred}} \Longrightarrow \Phi_3(x) = x^2 + x + 1$

$n=4$: $x^4 - 1 = (x^2+1)(x^2-1) = \underbrace{(x^2+1)}_{\Phi_4(x)}(x+1)(x-1)$

These are called the cyclotomic polynomials.

Fact $x^n - 1 = \prod_{d \mid n} \Phi_d(x)$.