From last time:

Thm: Given K/F the collection of all elems. of K which are algebraic over F is a subfield of K.

Ex: $K=\mathbb{C}$, $F=\mathbb{Q}$.

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

Then $\overline{\mathbb{Q}}$ is a field.

Also: $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$.

Thm: Suppose L is algebraic over K, and K is algebraic over F. Then L is algebraic over F.

Pf: Suppose $\alpha \in L$. Then α is alg. over K

$\Rightarrow \exists n \in \mathbb{N}, a_0, a_1, \dots, a_n \in K$ s.t. $\sum_{i=0}^{n} a_i \alpha^i = 0$.

Therefore

$[F(\alpha, a_0, \dots, a_n) : F(a_0, \dots, a_n)] < \infty$.

Also $[F(a_0, \dots, a_n) : F] < \infty$

so $[F(\alpha, a_0, \dots, a_n) : F] < \infty$

$\Rightarrow [F(\alpha) : F] < \infty$. ∎

$$\begin{array}{c}
F(\alpha, a_0, \dots, a_n) \\
\Big| {\scriptstyle <\infty} \\
F(a_0, \dots, a_n) \\
\Big| {\scriptstyle <\infty} \\
F(a_0, \dots, a_{n-1}) \\
\Big| {\scriptstyle <\infty} \\
\vdots \\
\Big| \\
F(a_0) \\
\Big| {\scriptstyle <\infty} \\
F
\end{array}$$

Composite fields

Def: Suppose $K_1, \dots, K_n \subseteq K$. The <u>composite field</u> (or <u>compositum</u>) $K_1K_2\cdots K_n$ is the smallest subfield of K containing all of them.

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

Thm: Suppose $K_1, K_2 \subseteq K$, $F \subseteq K_1, K_2$, $[K_1 : F] = m$, $[K_2 : F] = n$, $\{\alpha_1, \dots, \alpha_m\}$ is an F-basis for K_1, and $\{\beta_1, \dots, \beta_n\}$ is an F-basis for K_2. Then:

i) $K_1K_2 = \mathrm{span}_F\{\alpha_i\beta_j : 1 \le i \le m,\ 1 \le j \le n\}$

ii) $[K_1K_2 : F] \le mn$, with equality if and only if $\{\alpha_1, \dots, \alpha_m\}$ is lin. ind. over K_2.

Suppose now that K_1 and K_2 are finite extensions of F in K. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be an F-basis for K_1 and let $\beta_1, \beta_2, \ldots, \beta_m$ be an F-basis for K_2 (so that $[K_1 : F] = n$ and $[K_2 : F] = m$). Then it is clear that these give generators for the composite K_1K_2 over F:

$$K_1K_2 = F(\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_m).$$

Since $\alpha_1, \alpha_2, \ldots, \alpha_n$ is an F-basis for K_1 any power $\alpha_i{}^k$ of one of the α's is a *linear* combination with coefficients in F of the α's and a similar statement holds for the β's. It follows that the collection of linear combinations

$$\sum_{\substack{i=1,2,\ldots,n \\ j=1,2,\ldots,m}} a_{ij}\alpha_i\beta_j$$

what about closure under taking inverses?

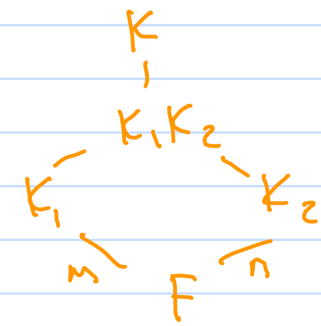
with coefficients in F is *closed* under multiplication and addition since in a product of two such elements any higher powers of the α's and β's can be replaced by linear expressions. Hence, the elements $\alpha_i\beta_j$ for $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, m$ *span* the composite extension K_1K_2 over F. In particular, $[K_1K_2 : F] \leq mn$. We summarize this as:

Proposition 21. Let K_1 and K_2 be two finite extensions of a field F contained in K. Then

$$[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$$

with equality if and only if an F-basis for one of the fields remains linearly independent over the other field. If $\alpha_1, \alpha_2, \ldots, \alpha_n$ and $\beta_1, \beta_2, \ldots, \beta_m$ are bases for K_1 and K_2 over F, respectively, then the elements $\alpha_i\beta_j$ for $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, m$ span K_1K_2 over F.

Proof: From $K_1K_2 = F(\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_m) = K_1(\beta_1, \beta_2, \ldots, \beta_m)$, we see as above that $\beta_1, \beta_2, \ldots, \beta_m$ span K_1K_2 over K_1. Hence $[K_1K_2 : K_1] \leq m = [K_2 : F]$ with equality if and only if these elements are linearly independent over K_1. Since $[K_1K_2 : F] = [K_1K_2 : K_1][K_1 : F]$ this proves the proposition.



Thm: Suppose $K_1, K_2 \subseteq K$, $F \subseteq K_1, K_2$,

$[K_1:F] = m$, $[K_2:F] = n$,

$\{\alpha_1, \dots, \alpha_m\}$ is an F-basis for K_1, and

$\{\beta_1, \dots, \beta_n\}$ is an F-basis for K_2. Then:

i) $K_1K_2 = \text{span}_F\{\alpha_i\beta_j : 1 \le i \le m, 1 \le j \le n\}$

ii) $[K_1K_2 : F] \le mn$, with equality if and only if

$\{\alpha_1, \dots, \alpha_m\}$ is lin. ind. over K_2.

Pf (our own proof):

i) $\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n \in K_1K_2 \Rightarrow F(\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n) \subseteq K_1K_2$

Also, $K_1, K_2 \subseteq F(\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n) \Rightarrow K_1K_2 \subseteq F(\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n)$.

So $K_1K_2 = F(\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n)$.

Note now that each of $\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n$ is <u>algebraic</u> over F, so $K_1K_2 = F(\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n)$ is also alg. over F. Therefore any element of K_1K_2 can be written as $f(\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n)$ for some $f \in F[x_1, \dots, x_m, y_1, \dots, y_n]$.

Each α_i^k is an F-lin comb. of $\alpha_1, \dots, \alpha_m$ since $K_1 = \text{span}_F(\alpha_1, \dots, \alpha_m)$. Similarly, each β_j^ℓ is an F-lin comb. of $\beta_1, \dots, \beta_n$.

Therefore $f(\alpha_1,\dots,\alpha_m,\beta_1,\dots,\beta_n)\in \mathrm{span}_F\{\alpha_i\beta_j : 1\le i\le m,\ 1\le j\le n\}$.

ii) $[K_1K_2:F]\le mn$ follows from i).

Note also that $K_1K_2=\mathrm{span}_{K_2}\{\alpha_1,\dots,\alpha_m\}$ (by the same argument used in i))

so $[K_1K_2:F]=[K_1K_2:K_2][K_2:F]$

$\le mn$, with equality

iff $\{\alpha_1,\dots,\alpha_m\}$ are K_2-lin ind. ∎

$$\begin{tikzcd} K_1K_2 \arrow[d, dash] \\ K_2 \arrow[d, dash] \\ F \end{tikzcd}$$

Exs:

1) $K=\mathbb{C}$, $F=\mathbb{Q}$, $K_1=\mathbb{Q}(\sqrt[3]{2})$, $K_2=\mathbb{Q}(i)$

$[K_1:\mathbb{Q}]=3$, $[K_2:\mathbb{Q}]=2$

$[K_1K_2:\mathbb{Q}]\le 6$, and

$[K_1:\mathbb{Q}],[K_2:\mathbb{Q}] \mid [K_1K_2:\mathbb{Q}]$

$\Rightarrow [K_1K_2:\mathbb{Q}]=6$.

$$\begin{tikzcd} & \mathbb{C} \arrow[d, dash] & \\ & K_1K_2 \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash] & \\ K_1 \arrow[dr, dash, "3"'] & & K_2 \arrow[dl, dash, "2"] \\ & \mathbb{Q} & \end{tikzcd}$$