Lecture 12:

F, K fields and $K \supseteq F$ (K extension of F).

Let $u \in K$: $F(u) \overset{\text{def.}}{=}$ intersection of all subfields of K containing F and u
$=$ smallest field containing F and u.

Def: $F(u)$ is a simple extension of F.

Def: $u \in K$ is algebraic over F if $p(u) = 0$ for some $0 \neq p(x) \in F[x]$, otherwise trancendental.

Ex: $\sqrt{2}$ algebraic over $\mathbb{Q}$: $p(x) = x^2 - 2$
$\sqrt{2}$ algebraic over $\mathbb{R}$: $p(x) = x - \sqrt{2}$
i algebraic over $\mathbb{R}$: $p(x) = x^2 + 1$
$\sqrt[3]{5} + 2$ algebraic over $\mathbb{Q}$: $p(x) = (x-2)^3 - 5$
π and e are transcendental over $\mathbb{Q}$

Theorem: $u \in K$ algebraic over F $\Rightarrow$ there exists a unique monic irreducible $p(x) \in F[x]$ with $p(u) = 0$. Moreover, if $g(x) \in F[x]$ and $g(u) = 0$, then $p(x) \mid g(x)$.

Proof: Let $S = \{g(x) \in F[x];\ g(u) = 0\}$. u alg. $\Rightarrow S \neq \emptyset$.
We use the w.o.a. on the degree in S and let $p(x) \in S$ be a monic polynomial of smallest degree.

$p(x)$ irr.: $p(x) = k(x)t(x) \Rightarrow p(u) = k(u)t(u) = 0_F \overset{F \text{ field}}{\Rightarrow}$ $k(u) = 0_F$ or $t(u) = 0_F$, and of smaller degree, contradiction!

$p(x) \mid g(x) \in S$: Div. alg $\Rightarrow g(x) = p(x)q(x) + r(x)$
$\Rightarrow r(u) = g(u) - p(u)q(u) = 0 - 0 \cdot q(u) = 0$,
and since $r(x)$ cannot be of smaller degree than $p(x)$, it follows that $r(x) = 0$, so $p(x) \mid g(x)$.

$p(x)$ unique: Let $t(x) \in S$, $t(x)$ monic and irreducible.
By above $p(x) \mid t(x) \overset{t(x) \text{ irr.}}{\Rightarrow} t(x) = c \cdot p(x),\ c \in F \overset{t(x) \text{ monic}}{\Rightarrow} t(x) = p(x)$. □

Def: The polynomial $p(x)$ above is called the minimal polynomial of u over F.

Ex: $x^2 - 2$ min. pol. of $\sqrt{2}$ over $\mathbb{Q}$
$x - \sqrt{2}$ min. pol. of $\sqrt{2}$ over $\mathbb{R}$

Theorem: Let $u \in K$ be algebraic over F, and let $p(x)$ be the minimal polynomial. Let $n = \deg p(x)$.
Then
1. $F(u) \cong F[x]/(p(x))$
2. $\{1, u, u^2, \dots, u^{n-1}\}$ is a basis of $F(u)$ over F.
3. $[F(u) : F] = n$

Proof: 1: $\{b_m u^m + \dots + b_1 u + b_0;\ b_i \in F, m \geq 0\} \subseteq F(u)$, so $f(u) \in F(u)$ for all $f(x) \in F[x]$. We define the function $\varphi : F[x] \to F(u)$ by $\varphi(f(x)) = f(u)$.

φ is a homomorphism of rings with $\ker\varphi = \{f(x) \in F[x];\ f(u) = 0\} =$
$= \{$all multiples of $p(x)\} =$ the ideal $(p(x))$

$\Rightarrow F[x]/(p(x)) \cong \operatorname{Im}\varphi$ (First Iso. Th.)

$p(x)$ irr. $\Rightarrow \operatorname{Im}\varphi \cong F[x]/(p(x))$ is a field containing F ($c \in F \Rightarrow \varphi(c) = c$) and the element u (since $\varphi(x) = u$). Since $\operatorname{Im}\varphi \subseteq F(u)$, it follows that $\operatorname{Im}\varphi = F(u)$ by the definition of $F(u)$.

2: Every $f(x) \in F[x]/(p(x))$ can be uniquely written
$f(x) = b_{n-1}x^{n-1} + \dots + b_1 x + b_0$, $b_i \in F$, which implies 2.

3 Follows from 2. □

Ex: $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(x^2-2) = \{a + b\sqrt{2};\ a, b \in \mathbb{Q}\}$
$\mathbb{R}(i) \cong \mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$

Corollary: If u and v have the same min. polynomial over F, then $F(u) \cong F(v)$.

Def: $K \supseteq F$ is called an algebraic extension of F if every $u \in K$ is algebraic over F.

Ex: $\mathbb{C}$ is an algebraic extension of $\mathbb{R}$: $a + bi$ is root of $(x-(a+bi))(x-(a-bi)) = x^2 - 2ax + (a^2+b^2) \in \mathbb{R}[x]$

Theorem: If K is a finite-dimensional extension field of F, then K is an algebraic extension of F.

Proof: Assume $[K:F] = n$ and let $u \in K$. If $u^i = u^j$, $0 \leq i < j$, then u is the root of $x^i - x^j \in F[x]$. Otherwise $\{1, u, u^2, \dots, u^n\}$ is $n+1$ different elements in K
$\Rightarrow$ lin. dependent over F $\Rightarrow$
$c_n u^n + \dots + c_1 u + c_0 = 0_F$ with some $c_i \neq 0$
$\Rightarrow u$ is a root of $c_n x^n + \dots + c_1 x + c_0 \in F[x]$.

Note: The converse is false in general.

Corollary: u algebraic over $F \Rightarrow F(u)$ alg. ext. of F

If $u_1, u_2, \dots, u_n \in K$, then $F(u_1, u_2, \dots, u_n) \overset{\text{def}}{=}$
$=$ intersection of all subfields of K containing F and all u_i $=$
$=$ smallest field containing F and all u_i.

Def: $F(u_1, u_2, \dots, u_n)$ is a finitely generated extension of F, generated by $u_1, u_2, \dots, u_n$.

Note: $F(u_1, u_2) = F(u_1)(u_2), \dots, F(u_1, u_2, \dots, u_n) = F(u_1, \dots, u_{n-1})(u_n)$
and $F \subseteq F(u_1) \subseteq F(u_1, u_2) \subseteq \dots \subseteq F(u_1, u_2, \dots, u_n)$.

Theorem: $K = F(u_1, u_2, \dots, u_n)$, all u_i alg. over F
$\Rightarrow$ K finite dimensional algebraic extension of F.

Proof: u_k alg. over F $\Rightarrow$ u_k alg. over $F(u_1, \dots, u_{k-1})$
$\Rightarrow$ $F(u_1, \dots, u_k) = F(u_1, \dots, u_{k-1})(u_k)$ fin. dim. over $F(u_1, \dots, u_{k-1})$ $\Rightarrow$

$$[K:F] = [F(u_1,\dots,u_n):F(u_1,\dots,u_{n-1})] \cdots [F(u_1,u_2):F(u_1)][F(u_1):F]$$

finite-dim. $\Rightarrow$ K alg. ext. of F. □

Ex: $\mathbb{Q}(\sqrt{3},\sqrt{5}) = \mathbb{Q}(\sqrt{3})(\sqrt{5})$. $x^2 - 3 \in \mathbb{Q}[x]$ min. ($\leftarrow$ irr.) pol. of $\sqrt{3}$ $\Rightarrow$ $[\mathbb{Q}(\sqrt{3}):\mathbb{Q}] = 2$. $x^2 - 5 \in \mathbb{Q}(\sqrt{3})[x]$ (irr. *) earlier exercise) min. pol. of $\sqrt{5}$ $\Rightarrow$ $[\mathbb{Q}(\sqrt{3})(\sqrt{5}):\mathbb{Q}(\sqrt{3})] = 2$

$$\Rightarrow [\mathbb{Q}(\sqrt{3},\sqrt{5}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{3})(\sqrt{5}):\mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}):\mathbb{Q}] = 2 \cdot 2 = 4$$

Basis $\{1, \sqrt{3}, \sqrt{5}, \sqrt{15}\}$.

Note: $\mathbb{Q}(\sqrt{3},\sqrt{5})$ is in fact a simple extension, $= \mathbb{Q}(\sqrt{3}+\sqrt{5})$: $\alpha = \sqrt{3}+\sqrt{5} \in \mathbb{Q}(\sqrt{3},\sqrt{5}) \Rightarrow \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{3},\sqrt{5})$.
Check that $\sqrt{3} = \frac{\alpha^3 - 14\alpha}{4}$, $\sqrt{5} = -\frac{\alpha^3 - 18\alpha}{4}$
$\Rightarrow$ $\mathbb{Q}(\sqrt{3},\sqrt{5}) \subseteq \mathbb{Q}(\alpha)$.

Note: K fin. dim. ext. of F $\Rightarrow$ K fin. gen. ext. of F, since if $\{u_1, \dots, u_n\}$ basis, then $K = F(u_1, \dots, u_n)$

Cor. $L \supseteq K \supseteq F$. L alg. ext. of K and K alg. ext. of F $\Rightarrow$ L alg. ext. of F

Proof: For $u \in L$: u alg. over K $\Rightarrow$
$a_m u^m + \dots + a_1 u + a_0 = 0_K$, $a_i \in K$ $\Rightarrow$
u alg. over $K_0 = F(a_1, \dots, a_m)$ $\Rightarrow$
$[K_0(u):K_0] < \infty$ by earlier th.
All a_i alg. over F $\Rightarrow$ $[K_0:F] < \infty$ by earlier theorem $\Rightarrow$ $[K_0(u):F] = [K_0(u):K_0]\cdot[K_0:F] < \infty$ $\Rightarrow$ u alg. over F by earlier theorem
$\Rightarrow$ L alg. ext. of F. □

Cor. $K \supseteq F$, $E = \{a \in K;\ a \text{ alg. over } F\}$
Then E field.

Proof: For $u, v \in E$: $F(u,v)$ is alg. ext. of F, in particular $u+v, uv, -u, u^{-1} \in F(u,v)$ are alg. over F $\Rightarrow$ $u+v, uv, -u, u^{-1} \in E$ $\Rightarrow$ E field.

Def: The field of algebraic numbers is E above when $K = \mathbb{C}$, $F = \mathbb{Q}$.