Last time: · Defined Unique Factorization (integral) Domains (UFDs)

· Proved: any PID is a UFD

In particular, $\forall$ field F, $F[x]$ is a UFD: any polynomial with coefficients in F can be written uniquely (up to order and multiplication by nonzero scalars) as a product of irreducibles

Recall If K, L are two fields and $K \subseteq L$ then K is a subfield of L and L is an extension of K.

Definition The degree $[L:K]$ of an extension $K \subseteq L$ is the dimension of L as a vector space over K.

$$[L:K] = \dim_K(L).$$

Ex $[\mathbb{C}:\mathbb{R}] = 2$, $[\mathbb{R}:\mathbb{Q}] = \infty$

Ex Let F be a field, $f \in F[x]$ irreducible, $E = F[x]/\langle f \rangle$. Then $[E:F] = \dim_F(F[x]/\langle f \rangle) = \deg f$.

Definition Let $F \subseteq L$ be a field extension. $\alpha \in L$ is algebraic over F if $\exists^{*}$ $p(x) \in F[x]$ s.t. $p(\alpha) = 0$ (in L).

Ex $\sqrt{2} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$:
$\sqrt{2}$ is a root of $x^2 - 2 \in \mathbb{Q}[x]$.

Ex $\sqrt[3]{4} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$:
$\sqrt[3]{4}$ is a root of $x^3 - 4 \in \mathbb{Q}[x]$.

Ex For any field F, $\alpha \in F$ is algebraic over F:
α is a root of $x - \alpha \in F[x]$.

Ex $i = \sqrt{-1} \in \mathbb{C}$ is algebraic over $\mathbb{Q}$: it's a root of $x^2 + 1 \in \mathbb{Q}[x]$.

Ex Let F be a field, $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$ irreducible. Then $\alpha = x + \langle f \rangle \in E := F[x]/\langle f \rangle$ is algebraic over F:

$$a_0 + a_1(x + \langle f \rangle) + \cdots + a_n(x + \langle f \rangle)^n = (a_0 + a_1 x + \cdots + a_n x^n) + \langle f \rangle = 0 + \langle f \rangle$$

$\Rightarrow \alpha$ is a root of $f(x) \in F[x]$.

Theorem 37.1 Let $F \subseteq E$ be a field extension. $\alpha \in E$ is algebraic over F $\Leftrightarrow$ $\exists$ a field K s.t. $F \subseteq K \subseteq E$ and $[K:F]$ is finite.

Moreover

1) The ideal $\{p \in F[x] \mid p(\alpha) = 0\} = \langle f \rangle$ for some irreducible polynomial $f \in F[x]$
2) The set $F[\alpha] := \{a_0 + a_1\alpha + \cdots + a_n\alpha^n \mid n \geq 0,\ a_0 \ldots a_n \in F\} \subseteq E$ is the smallest subfield of E containing F and α.
3) $[F(\alpha):F] = \deg f$.

Proof ($\Leftarrow$) Suppose $F \subseteq K \subseteq E$ and $[K:F] = \dim_F K = n$.
Consider $\{1, \alpha, \alpha^2, \ldots \alpha^n\}$. If $\alpha^i = \alpha^j$ for some $0 \leq i < j \leq n$ then $\alpha^{j-i} = 1$. $\Rightarrow \alpha$ is a root of $x^{j-i} - 1 = 0$.
Otherwise $\{1, \alpha, \ldots \alpha^n\}$ has $n+1 > \dim_F K$ elements
$\Rightarrow$ the set $\{1, \alpha, \alpha^n\}$ is linearly dependent over F:
$\exists\ a_0, \ldots a_n \in F$ s.t. $a_0 \cdot 1 + a_1\alpha + \cdots + a_n\alpha^n = 0$
$\Rightarrow \alpha$ is a root of $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$.
$\Rightarrow \alpha$ is algebraic over F.

($\Rightarrow$) Suppose $\alpha \in E$ is algebraic over F. Then $\exists\, q \in F[x]$, $q \neq 0$ s.t. $q(\alpha) = 0$. Consider the homomorphism

$$\varphi : F[x] \longrightarrow E, \quad \varphi(p) = p(\alpha).$$

Since $q \in \ker\varphi$ and $q \neq 0$, $\ker\varphi \neq 0$.

$\operatorname{Im}\varphi = \{ p(\alpha) \mid p \in F[x] \} = F[\alpha]$.

Since φ is a ring homomorphism, $F[\alpha]$ is a subring of E.

Since E is a field, $F[\alpha]$ is an integral domain.

By 1st iso theorem $F[\alpha] \cong F[x]/\ker\varphi$.

$\Rightarrow$ Since $F[\alpha]$ is an integral domain, $\ker\varphi$ is prime.

Since $F[x]$ is a PID, $\ker\varphi = \langle f \rangle$ for some $f \in F[x]$.

In $F[x]$, primes = irreducibles and ideals generated by irreducibles are maximal. $\Rightarrow F[\alpha] = F[x]/\langle f \rangle$ is a field.

Moreover, if $K \subseteq E$ is any subfield with $F \subseteq K$ and $\alpha \in K$ then $\forall\, a_0, \dots, a_n \in F$, $a_0 + a_1\alpha + \dots + a_n\alpha^n \in K$.

$\Rightarrow F[\alpha] \subseteq K$.

$\therefore$ $F[\alpha]$ is the smallest subfield of E containing F and α.

Finally $[F[\alpha] : F] = [F[x]/\langle f \rangle : F] = \deg f$. $\square$

Definition If $F \subseteq E$ and $\alpha \in E$ is algebraic over F then $f \in F[x]$ with $\langle f \rangle = \{ p \in F[x] \mid p(\alpha) = 0 \}$ is called (the) minimal polynomial of α. f is unique up to multiplication by units.

Note If $p \in F[x]$ is an irreducible polynomial with $p(\alpha) = 0$ then $p \in \langle f \rangle$. $\Rightarrow f \mid p$. But p is irreducible $\Rightarrow p = \text{unit} \cdot f$.

So, we may regard p as "the" irreducible polynomial of α

Remark If $p(x) \in F[x]$, $\deg p = 2$ or 3, and p has no roots in F then p is irreducible. This is because if

$p(x) = h(x) \cdot g(x)$ and $\deg h, \deg g < \deg p$

Then one of $h(x), g(x)$ has degree 1.

Now if $\deg h = 1$, $h(x) = a_0 + a_1 x$.

$\Rightarrow \alpha = -a_0 a^{-1}$ is a root of h. Contradiction

Ex $x^2 - 2 \in \mathbb{Q}[x]$ is irreducible since $\nexists \alpha \in \mathbb{Q}$ with $\alpha^2 = 2$. $\Rightarrow x^2 - 2$ is "the" minimal polynomial of $\sqrt{2} \in \mathbb{R}$

$\Rightarrow$ $x^3 - 2 \in \mathbb{Q}[x]$ is irreducible since $\nexists \beta \in \mathbb{Q}$ s.t. $\beta^3 = 2$. $\Rightarrow x^3 - 2$ is "the" minimal polynomial of $\sqrt[3]{2} \in \mathbb{R}$.

Q. Is $\sqrt[3]{2} \in \mathbb{Q}[\sqrt{2}]$?

A. If $\sqrt[3]{2} \in \mathbb{Q}[\sqrt{2}]$, then $\mathbb{Q}[\sqrt[3]{2}] \subseteq \mathbb{Q}[\sqrt{2}]$

$\dim_{\mathbb{Q}}(\mathbb{Q}[\sqrt[3]{2}]) = \deg(x^3 - 2) = 3$, $\dim_{\mathbb{Q}}(\mathbb{Q}[\sqrt{2}]) = \deg(x^2 - 2) = 2$

Since $3 \nmid 2$, $\mathbb{Q}[\sqrt[3]{2}] \not\subseteq \mathbb{Q}[\sqrt{2}]$

$\Rightarrow \sqrt[3]{2} \notin \mathbb{Q}[\sqrt{2}]$.