13.1 Fields and field extensions.

Question. If a polynomial $p(x) \in F[x]$ does not split into linear factors over F, can we find a 'minimal' field K containing F over which $p(x)$ splits?

Example.

- Every $p(x) \in \mathbb{C}[x]$ splits in $\mathbb{C} = \mathbb{R}\{1, i\}$.
- Not every $p(x) \in \mathbb{Q}[x]$ splits in $\mathbb{Q}\{1, i\} \leq \mathbb{C}$.
  Extensions of $\mathbb{Q}$ are ordered under inclusion. What does this ordered set look like?

Characteristic and prime subfield.
Every field F contains 1.

Definition. The *characteristic* of F, $\mathrm{ch}(F)$, is the smallest integer $p > 0$ such that $p \cdot 1 = 0$ if such a p exists; 0 otherwise.

The subfield of F generated by 1 is the smallest subfield of F, called the *prime subfield*.

Note: The prime subfield is not the ring generated by 1.
$\mathbb{Z}$ is a subring of $\mathbb{R}$, not a subfield.

Example.
$\mathrm{ch}(\mathbb{F}_p) =$ p for p prime, $\mathbb{F}_p = (\mathbb{Z}_p, +, \cdot)$
$\mathrm{ch}(\mathbb{R}) =$ 0

Theorem. *The prime subfield of a field F is either isomorphic to $\mathbb{Q}$ (and $\mathrm{ch}(F) = 0$) or isomorphic to $\mathbb{F}_p$ (and $\mathrm{ch}(F) = p$) for some prime p.*

Proof. $(\mathbb{Z}\cdot 1, +)$ is cyclic, hence isomorphic to $\mathbb{Z}$ or $\mathbb{Z}_n$ for some $n \in \mathbb{N}$.
In the first case, $\mathrm{ch}\, F = 0$ and the prime field of F is the field of fractions of $\mathbb{Z}$, i.e. $\mathbb{Q}$.
In the second case, suppose $n = a \cdot b$.
Then $0 = n \cdot 1 = (a1) \cdot (b1)$ implies $a = n$ or $b = n$.
Thus n is prime and $(\mathbb{Z}_n, +, \cdot)$ is a field. □

Note. if $\mathrm{ch}(F) = p > 0$, then $pa = 0$ for all $a \in F$.

Extensions.
Let $F \subseteq K$ be fields.
Then K is an F-vector space.
K is an *extension* of F, denoted K/F, of degree $[K : F] := \dim_F K$.
K/F is *finite* if $[K : F]$ is finite.

K from German "Körper"

Example.
$\mathbb{C}/\mathbb{R}$ is a degree 2 (i.e. finite) extension
$\mathbb{R}/\mathbb{Q}$ is an infinite extension.

Polynomial extensions.
Let $p(x) \in F[x]$ be irreducible (prime). Then

(1) $(p(x))$ is a maximal (prime) ideal in $F[x]$.
(2) $K := F[x]/(p(x))$ is a field.
(3) The canonical projection $\pi\colon F[x] \to K,\ f \mapsto f + (p)$, yields an embedding
$$F \hookrightarrow K,\ a \mapsto \bar{a}.$$
So we may view K as extension of F.
(4) $\bar{x}$ is a root of $p(y) \in K[y]$

Theorem. *Let $p(x) \in F[x]$ be irreducible over F of degree n, let $K := F[x]/(p(x))$. Then*
$$\bar{1}, \bar{x}, \bar{x}^2, \ldots, \bar{x}^{n-1}$$
is a basis for K over F, i.e.,
$$K = \{a_0 + a_1\bar{x} + \cdots + a_{n-1}\bar{x}^{n-1} \ :\ a_0, \ldots, a_{n-1} \in F\}.$$

Proof. Clearly $\operatorname{span}_F(1, \bar{x}, \ldots, \bar{x}^{n-1}) = K$

For lin independence suppose
$b_0 + b_1\bar{x} + \cdots + b_{n-1}\bar{x}^{n-1} = \bar{0}$ for $b_0, \ldots, b_{n-1} \in F$
$b_0 + b_1 x + \cdots + b_{n-1} x^{n-1} = \bar{0}$

Then $p(x) \mid b_0 + b_1 x + \cdots + b_{n-1} x^{n-1}$ yields $b_0 + b_1 x + \cdots + b_{n-1} x^{n-1} = 0$
since $\deg p(x) = n$. So $b_0 = \cdots = b_{n-1} = 0$. □

Example. $p(x) = x^3 - 2$ is irreducible over $\mathbb{Q}$. by Eisenstein

$K := \mathbb{Q}[x]/(x^3-2)$ is a field with $\bar{a} := a + (x^3-2)$ for $a \in \mathbb{Q}[x]$.

$\bar{x} \in K$ is a root of p $\quad x^3 \equiv 2 \mod p(x)$

$p(\underbrace{x + (x^3-2)}_{\bar{x}}) = p(x) + (x^3-2) = 0$ in K $\quad x^4 \equiv 2x$.

$K = \{ a_0 + a_1\bar{x} + a_2\bar{x}^2 \mid a_0, a_1, a_2 \in \mathbb{Q} \}$

Internal view.
For K/F and $\alpha, \beta, \dots \in K$,

$$F(\alpha, \beta, \dots)$$

denotes the smallest subfield of K containing F and $\alpha, \beta, \dots$, called the *field generated by* $\alpha, \beta, \dots$ over F.

$F(\alpha)$ is a *simple extension* of F; α is *primitive* for that extension.

Example. $\mathbb{C} = \mathbb{R}(i)$

Theorem. *Let $p(x) \in F[x]$ be irreducible and K/F with $\alpha \in K$ such that $p(\alpha) = 0$. Then*

$$F(\alpha) \cong F[x]/(p(x)).$$

Note. Any extension of F, which contains some root of $p(x)$, has a subfield isomorphic to $F[x]/(p(x))$.

Hence $F[x]/(p(x))$ is the smallest extension of F containing a root of $p(x)$.

Proof. Consider the ring hom

$\varphi: F[x] \to F(\alpha)$

$f(x) \mapsto f(\alpha)$

Then $p(x) \in \ker\varphi$.

Since p is irreducible, $(p(x))$ is maximal.

So either $\ker\varphi = (p(x))$ or $\ker\varphi = F[x]$.

The latter is impossible since $\varphi(F) = F \neq 0$.

Hence $\ker\varphi = (p(x))$.

$\varphi(F[x]) \cong F[x]/(p(x))$ is a field containing F and α.

So $\varphi(F[x]) = F(\alpha)$ and the Thm follows from the 1st Iso Thm. □

Ex. continued. $p(x) = x^3 - 2$ in $\mathbb{C}$ has roots $\sqrt[3]{2}$, $\sqrt[3]{2}\, e^{2\pi i/3}$, $\sqrt[3]{2}\, e^{4\pi i/3}$

Then $\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}(\sqrt[3]{2}\, e^{k2\pi i/3})$ as fields for $k = 1, 2$.