Thm. (Eisenstein's criterion)

If $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ and p is a prime s.t.

① $p \mid a_i$, for $0 \le i \le n-1$;

② $p \nmid a_n$;

③ $p^2 \nmid a_0$;

then $f(x)$ is irreducible over $\mathbb{Q}$.

(Proof.) We'll prove irreducibility over $\mathbb{Z}$.

§ $f(x) = \overset{\in \mathbb{Z}[x]}{(b_0 + b_1x + \cdots + b_rx^r)}\overset{\in \mathbb{Z}[x]}{(c_0 + c_1x + \cdots + c_sx^s)}$,

with $r, s < n$.

Then $a_0 = b_0c_0$ & $a_n = b_rc_s$.

$p \mid a_0$ & $p^2 \nmid a_0 \Rightarrow$ exactly one of b_0, c_0 is divisible by p

WLOG, $p \mid c_0$ & $p \nmid b_0$

Also, $p \nmid b_r$ and $p \nmid c_s$.

Now let $m = \min\{k \mid p \nmid c_k\}$. $1 \le m \le s$

$$a_m = \underset{\substack{\uparrow\\ p\nmid b_0}}{b_0}\,\underset{\substack{\uparrow\\ p\nmid c_m}}{c_m} + b_1\underset{\substack{\uparrow\\ p\mid c_{m-1}}}{c_{m-1}} + \cdots + b_m\underset{\substack{\uparrow\\ p\mid c_0}}{c_0}$$

So a_m is not divisible by p. $\therefore m = n$

But we had $m \le s < n$. ✱ ∎

Rmk. Now we can build an irred. polynomial of any degree we want.

e.g. $n=6$

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_6 x^6$$

$p=3$

$$6 - 9x + 12x^2 + 6x^3 - 15x^4 + 81x^5 - 7x^6$$

Ideals in $F[x]$, where F is a field

Thm. If F is a field, then every ideal in $F[x]$ is principal.

(Proof idea.) Take $I \subseteq F[x]$, let $p(x) \in I$ be a nonzero elt of minimal degree. Use division algorithm to show that $I = \langle p(x) \rangle$. ∎

Thm Let F be a field, pick $p(x) \in F[x]$. Then $\langle p(x) \rangle$ is a maximal ideal in $F[x]$ iff $p(x)$ is irred. over F.

(Proof.)

① Suppose $\langle p(x) \rangle$ is maximal.

Then $p(x)$ is nonconstant, b/c $\langle a \rangle = F[x]$, for any $a \in F$.

Also, $\langle p(x) \rangle$ is prime.

Now suppose $p(x) = a(x)\,b(x)$, for some non-constant $a(x), b(x) \in F[x]$.

Since $\langle p(x)\rangle$ is prime, either $a(x) \in \langle p(x)\rangle$ or $b(x) \in \langle p(x)\rangle$.

WLOG, $a(x) \in \langle p(x)\rangle$. But $p(x) = a(x)\,b(x)$, so $p(x) \in \langle a(x)\rangle$.

$\deg a(x) < \deg p(x) \Rightarrow \langle p(x)\rangle \subsetneq \langle a(x)\rangle$.

$\deg a(x) \neq 0 \Rightarrow \langle a(x)\rangle \subsetneq F[x]$.

So $\langle p(x)\rangle$ is not maximal. $\divideontimes$

② Suppose $p(x)$ is irreducible and consider an ideal $I \subseteq F[x]$ which contains $\langle p(x)\rangle$.

Prev. thm $\Rightarrow I = \langle f(x)\rangle$, for some $f(x) \in F[x]$.

$p(x) \in I \Rightarrow p(x) = f(x)\,g(x)$, for some $g(x) \in F[x]$.

$p(x)$ irred. $\Rightarrow \deg f(x) = 0$ OR $\deg g(x) = 0$

$\Downarrow$ $I = F[x]$

$\Downarrow$ $I = \langle p(x)\rangle$, b/c $p(x) = a \cdot f(x)$.

So $\langle p(x)\rangle$ is maximal. ▣

$1 \in R$
$\Rightarrow \langle 1\rangle = R$
$\forall r \in R$
$1 \cdot r \in \langle 1\rangle$
$r \cdot 1 \in \langle 1\rangle$

$a \in F, a \neq 0$
$a^{-1} p(x) \in F[x]$
$\therefore a \cdot a^{-1} p(x) \in \langle a\rangle$
$\therefore p(x) \in \langle a\rangle$

Extension fields

<u>Def</u>. A field E is an extension field of a field F if $F \subset E$ is a subfield.

<u>Ex</u>. Consider $F = \mathbb{Z}_2$. $p(x) = x^2 + x + 1$ is $\underbrace{\text{irred. over } F}$.

b/c it's quadratic, but has no roots

We want an extension field E of F s.t. $\exists\ \alpha \in E$ which is a root of $p(x)$.

Consider $E = F[x]/\langle p(x) \rangle$.

$p(x)$ irred.
$\Rightarrow \langle p(x) \rangle$ is maximal
$\Rightarrow E$ is a field.

$$\phi : F \hookrightarrow E$$
$$a \mapsto a + \langle p(x) \rangle$$

So $E \supset F$ is an extension field of F.

Consider $\alpha = x + \langle p(x) \rangle$.

$$\begin{aligned}
p(\alpha) &= (x + \langle p(x) \rangle)^2 + (x + \langle p(x) \rangle) + (1 + \langle p(x) \rangle) \\
&= (x^2 + \langle p(x) \rangle) + (x + \langle p(x) \rangle) + (1 + \langle p(x) \rangle) \\
&= (x^2 + x + 1) + \langle p(x) \rangle \\
&= p(x) + \langle p(x) \rangle \\
&= 0 + \langle p(x) \rangle = \text{zero elt in } E = F[x]/\langle p(x) \rangle
\end{aligned}$$

So $\alpha \in E$ is a root of $p(x)$.

> **Exercise.** Compute the four elements of E.

Thm. (Fundamental Theorem of Field Theory)

Let F be a field, $p(x) \in F[x]$ nonconstant. There exists an extension field of F which contains a zero of $p(x)$.

(Proof Idea.) Repeat the example:

0. Assume $p(x)$ is irreducible.
1. $E = F[x]/\langle p(x)\rangle$ is a field
2. $F \hookrightarrow E$ via $a \mapsto a + \langle p(x)\rangle$
3. $\alpha := x + \langle p(x)\rangle$ is a root of $p(x)$. ∎

Def. Let $E \supset F$ be an extension field.

1. $\alpha \in E$ is called algebraic over F if $\exists f(x) \in F[x]$ s.t. $f(\alpha) = 0$. Otherwise, α is transcendental over F.
2. E is called an algebraic extension if every elt. of E is algebraic
3. For any elements $\alpha_1, \ldots, \alpha_n \in E$, the smallest subfield of E containing F and $\alpha_1, \ldots, \alpha_n$ is denoted

$$F(\alpha_1, \ldots, \alpha_n).$$

"F extended by $\alpha_1, \ldots, \alpha_n$"

④ If $\exists\, \alpha \in E$ s.t. $E = F(\alpha)$, then E is called a simple extension of F.

Ex. $a \in \mathbb{Q}$ is algebraic over $\mathbb{Q}$ — $p(x) = x - a$

$\sqrt{2}, i \notin \mathbb{Q}$ are alg. over $\mathbb{Q}$ $\quad p(x) = x^2 - 2$

or $p(x) = x^2 + 1$

Most real #s are transcendental, though it's hard to check any particular number.

Thm. Let $E \supset F$ be an extension field, and suppose $\alpha \in E$ is algebraic over F. Then there is a unique irreducible, monic polynomial $p(x)$ of smallest degree for which α is a root, and if α is a root of $f(x) \in F[x]$, then $p(x) \mid f(x)$.