Theorem: (maximal ideals in $K[x]$)

Let K be a field. Then an ideal I of $K[x]$ is maximal if and only if $I = \langle p(x) \rangle$ where $p(x)$ is irreducible.

proof: $\Rightarrow$) Suppose I is maximal. By the previous lemma, $\exists\ p(x) \in K[x]$ with $I = \langle p(x) \rangle$. Suppose we may write

$$\boxed{p(x) = p_1(x) \cdot p_2(x)}$$

for $p_1(x), p_2(x) \in k[x]$.

Then

$$I = \langle p(x) \rangle \subseteq \langle p_1(x) \rangle$$

and

$$I \subseteq \langle p_2(x) \rangle$$

But I is maximal, so

either

$$\langle p_1(x) \rangle = k[x]$$

$\Rightarrow$ $p_1(x) \in k$ since

if $q(x) \in \langle p_1(x) \rangle$, $q(x) \neq 0$,

$$q(x) = p_1(x) \cdot q_1(x)$$

for some $q_1(x) \in k[x]$

$\Rightarrow \deg(g(x)) \geq \deg(p_1(x))$.

So if $\langle p_1(x) \rangle = k[x]$,

then $\langle p_1(x) \rangle$ contains

nonzero scalars $\Rightarrow$

$\langle p_1(x) \rangle = \langle 1_k \rangle$, and

$p_1(x) \in k$.

-or- $\langle p_1(x) \rangle = I$.

In this case, both

$p_1(x), p(x) \in I$

$p_1(x)$ cannot be a scalar

since $I \neq k[x]$.

But then

$$p_1(x) = p(x) \cdot q(x)$$ for

some $q(x) \in k[x]$ since

$$\langle p_1(x) \rangle = \langle p(x) \rangle = I.$$

We have

$$p_1(x) = p(x) \cdot q(x)$$
$$= p_1(x) \cdot p_2(x) \cdot q(x)$$

$\Rightarrow$ $\underline{p_2(x)}$, $q(x)$ are scalars

by degree considerations.

Therefore, $p(x)$ is irreducible.

$\Leftarrow$ Suppose $I = \langle p(x) \rangle$ and

$p(x)$ is irreducible. Let

J be an ideal,

$I \subseteq J \subseteq K[x]$.

We want to show either

$J = I$ or $J = K[x]$.

Suppose $J \neq I$.

We know $\exists$ $q(x) \in K[x]$,

$J = \langle q(x) \rangle$.

But $I \subseteq J$ and $I = \langle p(x) \rangle$,

so $p(x) = q(x) \cdot p_1(x)$

for some $p_1(x) \in K[x]$.

We know $p(x)$ is irreducible,

so either $q(x) \in K$

$\Rightarrow \langle q(x) \rangle = K[x]$

or $p_1(x) \in K$

$\Rightarrow \langle p(x) \rangle = \langle q(x) \rangle = J$,

contradiction.

Therefore, $J = K[x]$ and
$I = \langle p(x) \rangle$ is maximal. $\square$

Theorem: (Fundamental Theorem of Fields)

Let K be a field, $p(x) \in K[x]$.

Then $\exists$ an extension field L of K in which $p(x)$ has a zero: $\exists\ \alpha \in L$, $p(\alpha) = 0$.

proof: We may, upon factorization, assume $p(x)$ is irreducible

(Induction proof).

Let $\boxed{L = K[x]/\langle p(x) \rangle}$.

By the previous theorem, we know L is a field, and

K is isomorphic to a subring of L via the map

$$\beta \in K \mapsto \beta + \langle p(x) \rangle \in L.$$

Let $\boxed{\alpha = x + \langle p(x) \rangle} \in L$.

We want to show

$p(\alpha) = 0$. Here,

$$0 = 0 + \langle p(x) \rangle = \langle p(x) \rangle.$$

Suppose

$$p(x) = \sum_{i=0}^{n} \gamma_i x^i.$$

Then $p(\alpha) = \sum_{i=0}^{n} \gamma_i (x + \langle p(x) \rangle)^i$

$$= \sum_{i=0}^{n} \gamma_i (x^i + \langle p(x) \rangle)$$

$$= \left(\sum_{i=0}^{n} \gamma_i x^i \right) + \langle p(x) \rangle$$

$$= p(x) + \langle p(x) \rangle$$

$$= 0 + \langle p(x) \rangle$$

$$= \langle p(x) \rangle .$$

Therefore, $p(\alpha) = 0$!

$\square$

Fun Facts:

1) Gelfand-Schneider Theorem:

If a, b are algebraic over $\mathbb{Q}$, $b \notin \mathbb{Q}$, $a \notin \{0, 1\}$, then a^b is transcendental.

For example,

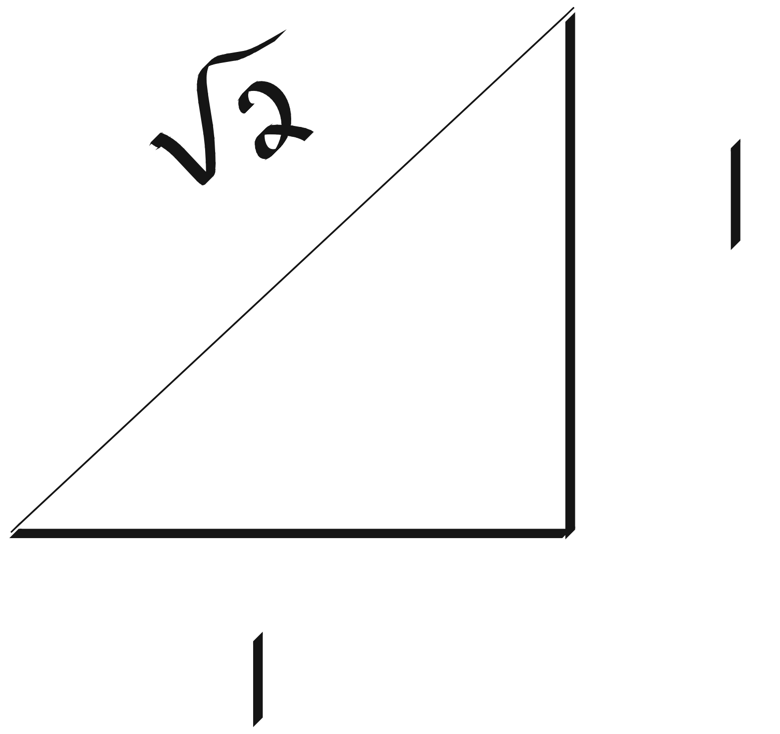
$3^{\sqrt{5}}$ is transcendental.

2) π and e are transcendental over $\mathbb{Q}$ (hard proofs, maybe Lindemann did both in 19th century?). One can show, without too much difficulty, that either $\pi + e$ or $\pi \cdot e$ is transcendental, but no one can prove which one it is! Open problem!

3) Constructibility Problems

Ancient Greek problems involving using a straightedge (unmarked ruler) and compass. For example, can we trisect and arbitrary angle using only straightedge and compass? All of these classical problems are proven false using field extensions!

Idea: the set of "constructible" numbers, starting with $\mathbb{Q}$, involves a series of degree-two extensions:



$\sqrt{2}$ is constructible

But, for example, trisecting angles give degree three extensions, so these are not, in general, constructible!

Characteristic of a Field

Recall: we showed that there is no field of order 6. Now we have the ability to prove such results in general!

Let K be a finite field. Then $(K, +)$ is an abelian group, so if $x \in K$, the order of x, considered in $(K, +)$, divides $|K|$.

Definition: The characteristic of a field K is the smallest $n \in \mathbb{N}$ such that $\forall\ x \in K$,

$$nx = \underbrace{x + x + x + \cdots + x}_{n \text{ times}} = 0_K .$$

If no such n exists, we say K is characteristic zero.

Theorem: (characteristic is prime or zero) Let k be a field. Then the characteristic of k is either zero or prime.

proof: Suppose k does not have characteristic zero, and let n denote its characteristic.

Suppose we can write

$n = m \cdot l$ for $1 < m, l < n$

(i.e., n is not prime).

Let $x \in K$, $x \neq 0_k$.

Then

$$0_K = nx = (m \cdot l)x$$

So either $m \cdot x = 0_K$ or $lx = 0_K$. By multiplying by x^{-1} (since K is a field), if, say, $m \cdot x = 0_K$, then $m \cdot 1_K = 0_K$.

But then if $y \in K$,

$$m \cdot y = m \cdot 1_K \cdot y = 0_K \cdot y = 0_K,$$

contradicting minimality of n.

Therefore, n is prime. $\square$