Eisenstein's Criterion

Let $\mathcal{R}$ be an integral domain and let
\[ f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \]
be a polynomial in $\mathcal{R}[x]$, for $n \geq 1$. Let $\mathcal{P}$ be
a prime ideal of $\mathcal{R}$. Suppose $a_0, \ldots, a_{n-1} \in \mathcal{P}$,
$a_0 \notin \mathcal{P}^2$. Then $f(x)$ is irreducible in $\mathcal{R}[x]$.

Proof: $f(x) = a(x)b(x)$ in $\mathcal{R}[x]$, $a(x), b(x)$ not units
(i.e., we're assuming $f(x)$ reducible). In
$$(\mathcal{R}/\mathcal{P})[x] \cong \mathcal{R}[x]/\mathcal{P}[x]$$
(Identify those rings) \text{ have }
\overline{a(x)b(x)} = x^n

since \overline{R/p} is an integral domain, both \overline{a(x)} and \overline{b(x)} have zero constant term

so otherwise the product is \overline{x^n} (check)

in other words, constant terms of \(a(x), b(x)\) are
in \(P\), thus constant term of \(\text{f(x)} = a(x)b(x)\) is
in \(P^2\), a contradiction.

\(\therefore \text{f(x)}\) is irreducible in \(R[x]\) \(\blacksquare\)

Application: Eisenstein's applied to \(Z[x]\)

Let \(p\) be a prime in \(Z\)

Let \(\text{f(x)} = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \in Z[x]\) for

\(n \geq 1\) and suppose \(p \mid a_i\) for \(0 < i < n\), but \(p^2 \nmid a_0\)

Then \(\text{f(x)}\) is irreducible in \(Z[x]\) (and \(Q[x]\))

(Gau\"{}s Lemma gives \( \cong Q[x]\) and then)

More Elementary Criterion

Prop: Let \(F\) be a field, and let \(p(x) \in F[x]\)

Then \(p(x)\) has a factor of degree \(1 \iff \exists a \in F\) s.t. \(p(a) = 0\) in \(F\).

Proof: Exercise using division algorithm.
Let \( F \) be a field \((1 \neq 0)\).

Examples we already know: \( \mathbb{Q} \), \( \mathbb{R} \), \( \mathbb{C} \), \( \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \).

\[
F(x_1, \ldots, x_n) = \left\{ \frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)} \middle| f(x_1, \ldots, x_n), g(x_1, \ldots, x_n) \in \mathbb{F}_p(x_1, \ldots, x_n); \quad g(x_1, \ldots, x_n) \neq 0 \right\}
\]

(Admittedly, equivalence classes)

Recall, for \( n \) a positive integer, \( 1 = 1_F \in F \)

\[
n \cdot 1 = \underbrace{1 + \cdots + 1}_n \quad (\text{or } -n \cdot 1 = \underbrace{-1 - 2 - \cdots - 1}_n)
\]

\( 0 \cdot 1 = 0_F \)

there is a ring homomorphism

\[
\mathbb{Z} \rightarrow F
\]

\[
m \mapsto m \cdot 1
\]

The kernel is either \((0)\) or \((p)\) for some prime \( p \in \mathbb{Z} \) (why? \( F \) an integral domain or 0).

If the kernel of the above is \((0)\), then say \( F \) has

**characteristic zero**.

If kernel is \((p)\) then \( F \) has **characteristic** \( p \).
Def: Let $S$ be a subset of $F$. The subfield of $F$ generated by $S$ is the smallest subfield containing $S$.

Def: The prime subfield of $F$ is the subfield generated by $\mathbb{F}_p$.

Remark: Prime subfield of $F$ is $\mathbb{F}_p$ iff $\text{char } F = p$.

Prime subfield of $\mathbb{F} F$ is $\mathbb{Q} \iff \text{char } F = 0$.

Now suppose $F$ is a subfield of a field $K$. Then we also write/say:

1. $K/F$
2. $K$ is an extension field of $F$
3. $F$ is a base field for $K$
4. $K/F$

Let $K$ be a field extension of $F$. Then $K$ is a vector space over $F$ (check). Write $[K:F]$ for the dimension of $K$ over $F$.

When $[K:F] < \infty$, say $K/F$ is a finite extension.

Call $[K:F]$ the degree of $K$ over $F$.

Review 4: $p(x) \in \mathbb{F}[x]$, $p(x)$ not a unit, $p(x) \neq 0$
Let $p(x)$ be an irreducible polynomial in $F[x]$. Then $F[x]/(p(x))$ is a field. Henceforth, we identify $F$ with its image in $F[x]/(p(x))$ and view $F[x]/(p(x))$ as a field extension of $F$.

**Def** Let $K/F$ be a field extension, let $p(x) \in F[x]$ be irreducible in $F[x]$, and let $\theta \in K$. We say that $\theta$ is a root of $p(x)$ if $p(\theta) = 0$ in $K$. (E.g., $i \in \mathbb{C}$ is a root of $x^2 + 1 \in \mathbb{R}[x]$.)
Then let \( p(x) \) be an irreducible polynomial in \( F[x] \).

Then there exists a field extension of \( F \) in which \( p(x) \) is a root.

**Proof**

Set \( K = F[x]/(p(x)) \) and take \( K/F \) a field extension as above. Consider the homomorphism as above

\[
F \rightarrow F[x]/(p(x)) = K
\]

with \( F \) identified with \( \bar{F} \).

Viewing \( F[x] \) via \( \bar{p} \) as a subring of \( K[x] \), we have \( \overline{p(x)} = a_n x^n + \ldots + a_0 \)

for \( a_n, \ldots, a_0 \in F \)

and

\[
\overline{p(x)} = \bar{p}(a_n) x^n + \ldots + \bar{p}(a_0) \in K[x]
\]

Now \( \overline{x} = x \mod (p(x)) \) in \( K = F[x]/(p(x)) \).

Then in \( K \)

\[
\overline{p(\overline{x})} = \bar{p}(a_n) \overline{x}^n + \ldots + \bar{p}(a_0)
\]

\[
= p(\overline{x}) \mod (p(x)) \text{ in } K
\]

\[
= 0 \text{ in } K
\]

E.g., \( F = \mathbb{Q} \), \( \overline{p(x)} = x^2 + 1 \)

\( K = \mathbb{Q}[x]/(x^2 + 1) \)
Def Let K be an extension field of F, and let \( \alpha_1, \ldots, \alpha_r \in K \). Then \( F(\alpha_1, \ldots, \alpha_r) \) is the subfield of K generated over F by \( \alpha_1, \ldots, \alpha_r \).

Example \( F = \mathbb{Q} \), \( p(x) = x^2 + 1 \)

\[ K = \mathbb{Q}[x] / (x^2 + 1) \]

Let \( L = \mathbb{Q}(i) \) in \( \mathbb{C} \) using the preceding notation.

Now consider the surjective ring homomorphism

\[ \mathbb{Q}[x] \rightarrow \mathbb{Q}[i] \]

where \( x \rightarrow i \)

Note \( \mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\} = \mathbb{Q}[i] \)

So we have \( \mathbb{Q}[x] \rightarrow \mathbb{Q}(i) \)

with kernel \( (x^2 + 1) \)

So \( \mathbb{Q}[i] \cong \mathbb{Q}[x] / (x^2 + 1) \)

Also, \( K \cong \mathbb{Q}(-i) = \mathbb{Q}[i] \)

Theorem Let \( p(x) \in F[x] \) be an irreducible polynomial of degree \( n(\geq 1) \), let \( K = F[x]/(p(x)) \)

and set \( \Theta = x \mod (p(x)) \) in \( K \). Then \( 1, \Theta, \ldots, \Theta^{n-1} \) form a basis for \( K \) as an \( F \)-vector space, and so \([K:F] = n\).