5. Polynomials

5.1 Polynomials

Polynomial ring -- Definition

Let R be a commutative ring. Then

$$R[x] = \{a_n \cdot x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 \ : \ a_i \in R\}$$

is called the *ring of polynomials over R*

Remainder theorem

Let F be a field, $a \in F$, and $f(x) \in F[x]$. Then $f(a)$ is the remainder in the division of $f(x)$ by $x - a$.

Factor theorem

Let F be a field, $a \in F$, and $f(x) \in F[x]$. Then a is a **zero** of $f(x) \iff x - a$ is a factor of $f(x)$.

- A polynomial of degree n over a field has at most n zeros, counting multiplicity.

Principal Ideal domain -- Definition

A principal ideal domain is an integral domain R in which every ideal has the form $\langle a \rangle = \{ra | r \in R\}$ for some $a \in R$.

- If F is a field then $F[x]$ is a principal ideal domain

Irreducibility

$f(x) \in F[x]$ is **reducible** over $F \iff f(x) = g(x)h(x)$ for some $g(x), h(x) \in F[x]$ of lower degree.
Otherwise f is **irreducible** over F

Irreducibility over $\mathbb{Q}$ and $\mathbb{Z}$

1. Let $f \in \mathbb{Z}[x]$ be irreducible $\Rightarrow f$ is irreducible over $\mathbb{Q}$.
   Contrapositive: if $f \in \mathbb{Z}[x]$ factors over $\mathbb{Q}$ then it factors over $\mathbb{Z}$
2. Let p be a prime and suppose that $f(x)[Z[x]$ with $deg f(x) > 1$. Let $\bar{f}(x)$ be the polynomial in $\mathbb{Z}_p[x]$ obtained from $f(x)$ by reducing all the coefficients of $f(x) \bmod p$.
   If $f(x)$ is irreducible over $\mathbb{Z}_p$ and $deg \bar{f}(x) = deg f(x) \Rightarrow f(x)$ is irreducible over $\mathbb{Q}$

Kronecker's Theorem

- Let F be a field
- Let $f(x)$ be a nonconstant polynomial in $F[x]$.
- Then there is an extension field E of F in which $f(x)$ has a 0

Proof

$f(x)$ has an irreducible factor $p(x)$. It's enough to construct a field E where $p(x)$ has a 0

Let's try $F[x]/\langle p(x) \rangle$ with the one-to-one mapping $\phi : F \to E; \phi(a) = a + \langle p(x) \rangle$

Let $p(x) = a_nx^n + ... + a_0$
Then

$$\begin{aligned} p(x + \langle p(x) \rangle) &= a_n((x + \langle p(x) \rangle)^n + ... + a_0 \\ &= a_n(x^n + \langle p(x) \rangle + ... + a_0 \\ &= a_nx^n + a_{n-1}x^{n-1} + ... + a_0 + \langle p(x) \rangle \\ &= p(x) + \langle p(x) \rangle \\ &= 0 + \langle p(x) \rangle \end{aligned}$$