Polynomial Rings

All rings in this note are commutative.

1. Polynomial Rings over Fields

Corollary: F is a field if and only if $F[x]$ is Principal Ideal Domain.

> *Sketch of a proof:* $\Longrightarrow$ follows because if F is a field then $F[x]$ is Euclidean Domain so gcd algorithm exists and every ideal is generated by gcd of all the generators $\Longrightarrow F[x]$ is Principal Ideal Domain.
> $\Longleftarrow F[x]$ is a Principal Ideal Domain then (x) is prime ideal.

$(x) =$ polynomials in $F[x]$ with 0 constant terms
$p(x)q(x)$ has constant term $p(0)q(0)$
If $p(x)q(x)$ has 0 constant term then $p(0) = 0$ or $q(0) = 0$ and hence $p(0) \in (x)$ or $q(0) \in (x)$.
$\Longrightarrow (x)$ is maximal $\Longrightarrow F[x]/(x)$ is a field but $F[x]/(x) \cong F$

$$F[x] \xrightarrow[\text{evaluate } p(x) \text{ at } 0]{\phi} F$$

$$F \cong F[x]/\ker\phi = F[x]/(x)$$

Proposition: The maximal ideals in $F[x]$ are the ideals $(f(x))$ generated by irreducible polynomials of $f(x)$. In particular, $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible.

2. Properties of Ideals

Proposition: Assume R is commutative with identity 1.

(1) The ideal I is a maximal ideal if and only if the quotient ring R/I is a field.

(2) The ideal I is a prime ideal in R if and only if the quotient ring R/I is an integral domain.

> *Sketch of a proof:* I is prime ideal if and only if $I \neq R$ and whenever $ab \in I$, then either $a \in I$ or $b \in I$.
> R/I is an integral domain if $(r + I)(s + I) = I$ then either $r + I = I$ or $s + I = I$ (where $r + I = I$ means $\overline{r} = \overline{0} = \overline{I}$).
> Assume I is prime ideal then
>
> $$I = (r + I)(s + I) = \{\underbrace{(r + a)(s + b)}_{= rs+rb+as+ab} : a, b \in I\}$$
>
> $\Longrightarrow rs \in I$ because $rs + rb + as + ab \in I$ and $rb, as, ab \in I$.
> $\Longrightarrow r \in I$ or $s \in I$ because I is prime ideal.
> $\Longrightarrow r + I = I$ or $s + I = I \Longrightarrow R/I$ is an integral domain.
> If R/I is an integral domain then for $a, b \in I$
>
> $$ab + I = (a + I)(b + I) = I$$
>
> since R/I is integral domain then either $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$.

Corollary: Every maximal ideal of R is a prime ideal.

Proposition: If R is a Principal Ideal Domain then I is prime ideal implies I is maximal ideal.

Definition: Let R be an integral domain. The nonzero element $p \in R$ is called *prime* in R if the ideal (p) generated by p is a prime ideal.

Propsition: If I is prime ideal and R is a prime then $I = (p)$.

Sketch of a proof: I is contained in a maximal ideal $I = (p) \subseteq (m) \subsetneq R$ ($p \in (m) = \{bm : b \in R\}$).
If $p = am$ for some $a \in I$ then $am \in I$ so $a \in I$ or $m \in I = (p)$.
If $m \in I$ then $I = (p) = (m)((m) \subseteq (p))$ so I is maximal ideal.
If $a \in I$ then $a = rp$ so $p = am = (rp)m \Longrightarrow p - p \cdot r \cdot m = p(1 - r \cdot m) = 0$ then $1 - rm = 0$ or m is a unit.
If m is a unit, then $(m) = R$. *Contradiction!*
Conclude I is maximal ideal.

3. Polynomials in Several Variables over a Field

$$\underset{field}{F} \subseteq \underset{P.I.D.}{F[x]} \subseteq \underset{not\ a\ P.I.D.\ in\ general}{F[x,y] \subseteq F[x,y,z]}$$

Example:

Ideals: $(0) \neq F$, $(p(x))$ and $(f_1(x,y), f_2(x,y), \cdots f_n(x,y))$

Definition: A commutative ring R with 1 is called *Noetherian* if every ideal of R is finitely generated.

Theorem: (*Hilbert's Basis Theorem*) All monomial ideal in $F[x_1, \cdots, x_n]$ are Noetherian if F is a field. If R is a Noetherian ring then so is the polynomial ring $R[x]$.

Sketch of a proof: $p(x) = 1 \cdot x^n + a_{n-1} \cdot x^{n-1} + a_{n-2} \cdot x^{n-2} + \cdots + a_0$
$F[x]/(p(x))$ can be thought of as a vector space over F has as basis $\{1, x, x^2, \cdots, x^{n-1}\}$.
If $g(x) \subseteq F[x]$ where $g(x) = p(x)q(x)+r(x)$ such that $\deg(r(x)) < \deg(p(x)) \Longrightarrow g(x) \in r(x)+(p(x))$
$g(x) + (p(x)) = r(x) + (p(x))$

Example:

$F[x]/(x) = \mathcal{L}_F\{1\}$
$\mathbb{Z}_2[x]/(x^2 + x + 1) = \{0, 1, x, x+1\} = \mathcal{L}_2\{1, x\}$

Example:

$x^3 + 1 = p(x)$

$$\begin{aligned} F[x]/(x^3+1) &= \mathcal{L}_F\{1, x, x^2\} \\ x^4 &= x(x^3+1) - x \\ x^4 + (p(x)) &= -x + (p(x)) \end{aligned}$$

There is no unique division algorithm when you work over polynomial rings with more variables

$$x^2 + y^2 - 1 \qquad \text{and} \qquad x^4 - y + 2$$

$\Longrightarrow$ Next best thing is to put an order on the monomials and cancel the *largest* terms.

Note that Hilbert's Basis Theorem shows how larger Noetherian rings may be built from existing ones in a manner analogous to the theorem given below.
Theorem: R is a Unique Factorization Domain if and only if $R[x]$ is a Unique Factorization Domain.