Polynomial Rings

All rings in this note are commutative.

Example:

$$f_1 = y^2 - 3x + y + 5$$
$$f_2 = -y^2 + 2x + y - 1$$
$$g = -4y^2 + x + 18y + 24 \in \mathcal{L}\{f_1, f_2\}$$
$$g = af_1 + bf_2 \qquad\qquad [g]_{\{f_1,f_2\}}$$

$$\begin{aligned} a - b &= -4 \\ -3a + 2b &= 1 \\ a + b &= 18 \end{aligned}$$

$$\begin{bmatrix} 1 & -1 \\ -3 & 2 \end{bmatrix}^{-1} \begin{bmatrix} -4 \\ 1 \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix} \qquad \Longrightarrow \qquad a = 7, b = 11$$

1. Chinese Remainder Theorem

Definition: The ideal A and B of ring R are said to be *comaximal* if $A + B = R$ (means relatively prime).

Theorem: *(Chinese Remainder Theorem)* Let $A_1, A_2, \cdots, A_k$ be ideals in R. The map

$$R \longrightarrow R/A_1 \times R/A_2 \times \cdots \times R/A_k \qquad \text{defined by} \qquad r \longmapsto (r + A_1, r + A_2, \cdots, r + A_k)$$

is a ring homomorphism with kernel $A_1 \cap A_2 \cap \cdots \cap A_k$. If for each $i, j \in \{1, 2, \cdots, k\}$ with $i \neq j$ the ideals A_i and A_j are comaximal, then this map is surjective and $A_1 \cap A_2 \cap \cdots \cap A_k = A_1 A_2 \cdots A_k$, so

$$R/(A_1 A_2 \cdots A_k) = R/(A_1 \cap A_2 \cap \cdots \cap A_k) \cong R/A_1 \times R/A_2 \times \cdots \times R/A_k.$$

Sketch of proof: If A_1 and A_2 are pairwise comaximal then

$$A_1 \cap A_2 = A_1 \cdot A_2$$
$$A_1 \cap A_2 \subseteq A_1 \cdot A_2$$
$$A_1 \cdot A_2 \subseteq A_1 \cap A_2 \text{ (clear for P.I.D.)}$$

$$(a_1 r_1 + a_2 r_2 + \cdots + a_n r_n)(b_1 r_1' + b_2 r_2' + \cdots + b_n r_n')$$
$$\sum_{i=1}^{n} \sum_{j=1}^{m} a_i r_i b_j r_j' \in A_1 \text{ and } A_2$$
$$A_1 + A_2 = R$$
$$x \in A_1, y \in A_2 \text{ such that } x + y = 1$$
$$c \in A_1 \cap A_2 \text{ then } c = c \cdot 1 = cx + cy \in A_1 A_2$$

Example:

$$x \cong 2(\text{mod } 3)$$
$$x \cong 3(\text{mod } 5)$$
$$x \cong 2(\text{mod } 7)$$

$$R = \mathbb{Z} \qquad A_1 = (3) \quad A_2 = (5) \quad A_3 = (7) \qquad A_1 \cap A_2 \cap A_3 = (105)$$

Example:

$$(10) + (13) = (\gcd(10, 13)) = (1) = \mathbb{Z} \qquad\qquad (10) \cap (13) = (130) = (10) \cdot (13)$$

comaximal

$-5 \cdot 10 + 4 \cdot 13 = 2$

$-9 \cdot 10 + 7 \cdot 13 = 1$

$(10) + (13) = (\gcd(10, 13)) = (1) = \mathbb{Z}$ $\qquad$ $(10) \cap (13) = (130) = (10) \cdot (13)$

not comaximal because the gcd is not 1

$(x^3 + 1) + (x^2 + 2x + 1) = (x + 1)$ $\qquad$ $(x^3 + 1) \cap (x^2 + 2x + 1) = (x^4 + x^3 + x + 1)$

not comaximal

Generalization says: If A_i and A_j are comaximal then $A_1 \cap A_2 \cap \cdots \cap A_k = A_1 A_2 \cdots A_k$.

2. Polynomial Rings over Fields

Corollary: If F is a field, then $F[x]$ is a Principle Ideal Domain and is a Unique Factorization Domain.

The quotient $F[x]/I$ always looks like $I = (p(x))$, where F is a field and $p(x)$ is a polynomial in $F[x]$.

Proposition: Let $p(x)$ be a nonconstant element of $F[x]$ and let

$$p(x) = f_1(x)^{a_1} f_2(x)^{a_2} \cdots f_k(x)^{a_k}$$

be its factorization into irreducibles, where the $f_i(x)$ are distinct. Then the following isomorphism of rings:

$$F[x]/(p(x)) \cong F[x]/(f_1(x)^{a_1}) \times F[x]/(f_2(x)^{a_2}) \times \cdots \times F[x]/(f_k(x)^{a_k}).$$

$F[x]/(p(x))$ has as unique elements of quotient ring $a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + (p(x))$.

Example:

$F[x]/(x^2 + 1)$ has elements of the form $a + bx + (x^2 + 1)$

$$\begin{aligned}(a + bx + (x^2 + 1))(c + dx + (x^2 + 1)) &= ac + bcx + adx + bdx^2 + (x^2 + 1) \\ &= ac + bcx + adx - bd + (x^2 + 1)\end{aligned}$$

$bdx^2 = bdx^2 + bd - bd = bd(x^2 + 1) + (-bd)$

$r - s \in I$ then $r \equiv s$ in $R/I \implies r - s \equiv 0$ in R/I.

3. Polynomials in Several Variables over a Field

In general, the polynomial ring $F[x_1, \cdots, x_n]$ is a Unique Factorization Domain however, it is *not* a Principle Ideal Domain unless $n = 1$.

Example:

If $F[x, y](x, y^4)$ is not generated by a single polynomial

$2x + 3y^4 \in (x, y^4)$
$x^2 + 3y^5 \in$
there is no single polynomial which divides both $2x + 3y^4$ and $x^2 + 3y^5$.

Theorem: (*Hilbert's basis theorem*) If R is a Noetherian ring then the polynomial ring $R[x]$ is also Noetherian, where R is Noetherian means its every ideal is finitely generated.

Example:

$F[x_1, x_2, \cdots]$ is not Noetherian because $I = (x_1, x_2, \cdots)$ needs to be generated by all x_i.

In $F[x_1, x_2, \cdots, x_n]$ the elements look like $\sum_{\alpha} c_{\vec{\alpha}} \vec{x}^{\vec{\alpha}} = p(\vec{x})$ where $x^{\vec{\alpha}} = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ and $c_{\vec{\alpha}} \in F$

degree of a polynomial $p(\vec{x}) = \max_{\alpha} c \sum_{i=1}^{n} \alpha_i$.

$F[x_1, x_2, \cdots, x_n]$ is the ring of formal power series where we allow infinite sums.