MATH 250A LECTURE RECAPS (POLYNOMIAL RINGS)

PATRICK OARE

Unless otherwise specified, assume all rings are commutative, and that R is a (commutative) ring.

1. 10/17 (Polynomials, Irreducibility)

- If a polynomial $f \in R[X]$ has leading coefficient 1, we say f is **monic**.
- **Division with remainder**: Let $f, g \in R[X]$, f monic. Then $\exists q, r \in R[X]$ such that $deg(r) < deg(f)$ or $deg(r) = -\infty$ such that:
$$g(x) = f(x)q(x) + r(x)$$
This implies that for a field K, $K[X]$ **is Euclidean** since we can assume all polynomials are monic.
- **Finding primes**: For finding prime integers, we may use the Sieve of Eratosthenes: we list all of the integers in order of size, and cross off all multiples of each integer as we pick new prime ones. We may use this for polynomials; order them in terms of degree, and cross off all multiples. For the ring $\mathbb{F}_2[X]$, we may do this to find primes in $x, x+1, x^2+x+1, x^3+x+1, ...$
- **Roots**: Suppose a is a root of $f \in R[X]$. Then we may write:
$$f(x) = g(x)(x-a)$$
for some $g \in R[X]$. To show this, just divide by $(x-a)$ and show the remainder must be 0. An important corollary of this is that **any polynomial f of degree n over an integral domain has at most n roots**. For example, $\mathbb{Z}/8\mathbb{Z}$ has 4 roots– $1, 3, 5, 7$– to the polynomial $x^2 - 1$, which has degree 2.
- **Multiplicative Groups of Fields**: A generator of $(\mathbb{Z}/p\mathbb{Z})^*$ is called a **primitive root**. We show that **for any field F, any finite subgroup of F^* is cyclic**. We show this for $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Let R be the ring $\mathbb{Z}/p\mathbb{Z}$, and let $G = R^*$. $R[X]$ is Euclidean and hence integral, so $x^n - 1$ has $\leq n$ roots in R for any $n \in \mathbb{N}$. Then G has $\leq n$ elements x of order n for each $n \in \mathbb{N}$ as there are $\leq n$ roots of this polynomial in R. But then the result follows from this lemma:

  Lemma 1.1. If G is a finite abelian group with $\leq n$ elements of order n for all $n \in \mathbb{N}$, then G is cyclic.

  Proof. Since G is finite and abelian, $G \cong \oplus_{i=1}^m \mathbb{Z}/p_i^{n_i}\mathbb{Z}$. If some $p_i = p_j$ for $i \neq j$, then G has $p_i^2 - 1$ elements of order p_i, , contradicting our assumption, so all the p_i are distinct. But $\mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/b\mathbb{Z} \cong \mathbb{Z}/ab\mathbb{Z}$ if a and b are coprime, and so this proves the assertion. □

- **Content**: Let R be a UFD with field of fractions K, and let $f \in K[X]$. As an example, if $f \in \mathbb{Z}[X]$, then the content of f is the gcd of its coefficients. If not, let $f(x) = \sum_{i=0}^{n} a_i x^i$. The idea behind defining the **content** $c(f) \in K$ is that we want:
$$\frac{f(x)}{c(f)}$$
to be a rescaling of f with integer coefficients such that the coefficients share no common factor.

  We define the content. For each prime p, $a_i = p^{m_i} b_i$ with p not dividing the numerator or denominator of b_i and $m_i \in \mathbb{Z}$. Note that the m_i's can be negative, which is crucial. Then, we take:
$$c(f) := p^{\min\{m_i\}_{i=1}^{n}} \times b$$
where b is a rational with p not dividing the numerator or the denominator.

  For example, consider $f(x) = \frac{2}{3}x^2 + 4$. For $p = 2$, $a_2 = \frac{2}{3} = 2^1 \times \frac{1}{3}$ and $a_0 = 4 = 2^2 \times 1$, so the min m_i is 1, and thus $c(f) = 2b$ for some rational b with p not dividing the numerator or the denominator of b. For $p = 3$, $a_2 = 3^{-1} \times 2$, so $m_2 = -1$ and $a_0 = 3^0 \times 4$, so $m_0 = 0$. However, $m_2 < m_0$, so $c(f) = 3^{-1}b$ for a different b. Putting these together, we see $c(f) = \frac{2}{3}$.
- **Gauss's Lemma**: If $f, g \in \mathbb{Q}[X]$, then:
$$c(fg) = c(f)c(g)$$
We may write $f = c(f)f'$ and $g = c(g)g'$ where $c(f') = 1 = c(g')$, so we must only prove this for $c(f) = 1 = c(g)$. Note that $c(f) = 1 \implies f \in \mathbb{Z}[X]$ with coprime coefficients. Let p be a prime. Then p does not divide every coefficient of f and g because the content is 1– let a_i and b_j be the first coefficients not divisible by p. But:
$$(fg)(x) = ... + (a_0 b_{i+j} + ... + a_i b_j + ... + a_{i+j} b_0)x^{i+j}$$
and each coefficient other than $a_i b_j$ is divisible by p, so the total coefficient is not divisible by p, and thus $p^{min\{m_i\}} = 1$, so the total content is 1.
- Let $K = Frac(R)$. The irreducibles of $R[X]$ are either:
  (1) Degree 0. The irreducibles of R.
  (2) Degree > 0. The irreducibles of $K[X]$ with content 1
- **Theorem**: If R is a UFD, then $R[X]$ is.

  This just follows from defining the content similar to what we did before (except now only defined up to a unit). We can then prove that irreducible implies prime and that any polynomial can be factored into a product of irreducibles, and that $K[X]$ is a UFD (it is Euclidean).
- **Testing for Irreducibility**:
  - Reduction modulo p. If $f(x) = g(x)h(x)$ is reducible, then $f(x) = g(x)h(x) \mod p$. So, if we reduce $f(x) \mod p$ and can reduce it mod p, then we can reduce it. For example, consider $9x^4 + 6x^3 + 26x^2 + 13x + 3$. Reducing mod 2, we get $x^4 + x + 1 \mod 2$, which is irreducible mod 2. Thus, this is irreducible.

As another example, consider $x^4 - x^2 + 3x + 1$. Reducing mod 2, this is $(x+1)(x^3 + x^2 + 1) \mod 2$, where both of these are irreducible mod 2. We can also reduce it to $(x^2+1)^2 \mod 3$, and these are incompatible.

– **Eisenstein's Criterion**: Suppose $f(x) \in \mathbb{Z}[X]$ has the following properties:
  (1) f is monic, or p does not divide the leading coefficient.
  (2) All other coefficients are divisible by p.
  (3) The constant term is **not** divisible by p^2.

  Then f is irreducible in $\mathbb{Z}[X]$.
  We can also make a change of variables (i.e. to $z := x - 1$). Then, if $f(z)$ is irreducible by Eisenstein, so if $f(x)$. This is helpful for showing that $x^{p-1} + x^{p-2} + ... + x + 1$ is irreducible. This works because p splits as a prime power in the cyclotomic ring $\mathbb{Z}[\xi]$, for $\xi := exp(2\pi i/p)$

2. 10/19 (Hilbert's Theorem, Symmetric Functions)

- **Rational Root Theorem**: Let $a_n x^n + ... + a_0 \in \mathbb{Q}[X]$ (this applies equally as well to $\mathbb{Z}$). Then, the only rational roots to this equation are of the form $\frac{c}{d}$, with $c|a_0$ and $d|a_n$. In particular, if $f \in \mathbb{Z}[X]$ is monic, then any linear factor is of the form $(x - b)$, with $b|f(0) = a_0$.
- Any polynomial of degree ≤ 3 with no linear factors is irreducible. In particular, combining this with the rational root test makes it easy (for small values of coefficients) to check if polynomials of degree ≤ 3 are irreducible.
- Unexpected factorizations. Consider the following polynomials:
  (1) $x^{100} + 1$. This is divisible by $x^4 + 1$, so it is reducible.
  (2) $x^{100}+2$. This is irreducible by Eisenstein for $p = 2$. Note that Eisenstein makes it easy to give examples of polynomials of large degrees: just take $x^n + p$.
  (3) $x^{100} + 4$. This one has the factorization $(x^{50} + 2x^{25} + 2)(x^{50} - 2x^{25} + 2)$.
- **Hilbert's Theorem**: Let K be a field. Then, any ideal of $K[x_1, ..., x_n]$ is finitely generated.
- Generation as an ideal and generation as a ring are different: The ideal (x) in $K[X, Y]$ is generated by one element as an ideal, but if we consider it to be a ring without identity, then (x) has no finite set of generators: indeed, one set of generators is $\{x, xy, xy^2, xy^3, ...\}$.
- **Noetherian Rings**: A ring R is **Noetherian** if every ideal of R is finitely generated. We have:

  Theorem 2.1. If R is a ring, TFAE:
  (1) R is Noetherian.
  (2) Every nonempty set of ideals has a maximal element.
  (3) Every strictly increasing chain $I_1 \subseteq I_2 \subseteq ...$ stabilizes.

  To prove this, we show that $ii \iff iii$, which is just a general statement about partially ordered sets. Then, we show that $i \iff iii$. Note that we can equally define a Noetherian ring as a ring where every increasing chain of ideals stabilizes. Likewise, we can define the notion of an **Artinian ring**: this is one where every

decreasing set of ideals stabilizes. $\mathbb{Z}$ is not Artinian; consider the ideals generated by 2^n for $n \in \mathbb{N}$.

- **Noether's Theorem**: If R is Noetherian, then $R[X]$ is Noetherian.

  To prove this, we take an ideal $I \subset R[X]$ and associate a chain $I_0 \subseteq I_1 \subseteq ...$ in R, where I_0 is the leading coeffs of polynomials in I of degree ≤ 0, and so on. Clearly this is an increasing chain, so it stabilizes at some $m \in \mathbb{N}$. Then, pick a set of generators for each $I_0, I_1, ..., I_m$ and union it together– this will be finite as R is Noetherian, so each I_i is finitely generated. This set is a set of generators for I.
- **Rings of Invariants**: Let G be a group acting on a K-vector space V with basis $\{x_1, ..., x_n\}$. Then $g \cdot x_1 = g_{11}x_1 g_{12}x_2 + ... + g_{1n}x_n$ for $g_{1i} \in K$, and more generally:

$$g \cdot x_i = \sum_{j=1}^{n} g_{ij}x_j$$

  for coefficients $g_{ij} \in K$. If p, q are polynomials over $\{x_1, ..., x_n\}$, then $g \cdot (p + q) = g \cdot p + g \cdot q$, and $g \cdot (pq) = (g \cdot p)(g \cdot q)$, so the action preserves structure. We define the **ring of invariants** as the set of polynomials fixed by the action from G.
- **Symmetric Functions**: In the previous example, take $G := S_n$ to be the symmetric group on n elements with the obvious action on the polynomials (i.e. permutes the basis vectors). A **symmetric function** is an invariant polynomial under the action of S_n. For example, take $x_1 + ... + x_n$, or take something like:

$$x_1x_2 + x_1x_3 + ... + x_1x_n + x_2x_3 + ... + x_2x_n + ... + x_{n-1}x_n$$

  Essentially, we can take a monomial and sum over all other monomials of the same length. Consider the polynomial:

$$\prod_{i=1}^{n}(X - x_i) = X^n - (\sum_{i=1}^{n} x_i)X^{n-1} + (\sum_{i<j} x_ix_j)X^{n-2} + ... + \prod_{i=1}^{n} x_i$$

  These coefficients are called the **elementary symmetric functions**. To find these, just take each length between 1 and n and sum all the monomials of that length.
- **Fundamental Theorem of Symmetric Polynomials**: Let the elementary symmetric polynomials be $e_1, ..., e_n$. Then every symmetric polynomial is a polynomial in $e_1, ..., e_n$.

  To prove this, suppose p is a symmetric polynomial. Take the largest monomial with lexicographical ordering $ax_1^{n_1}x_2^{n_2}...x_m^{n_m}$ with $n_1 \geq n_2 \geq ....$ Such an ordering of the n_i exists because this polynomial is symmetric, and so contains all combinations of the n_i. Then take:

$$q := (x_1 + ... + x_n)^{n_1 - n_2}(x_1x_2 + ...)^{n_2 - n_3}...(x_1x_2x_3...)^{n_{m-1} - n_m}$$

  The polynomial $p - aq$ has a smaller largest monomial, and we cannot have an infinite sequence of decreasing polynomials, so this completes the proof.

3. 10/24 (Symmetric Polynomials, Invariants)

- **Newton's Identities**: How do we decompose $\sum_i x_i^4$ into symmetric polynomials? Recall:

$$\prod_{i=1}^{n}(x - x_i) = x^n - e_1x^{n-1} + e_2x^{n-2} + ...$$

We take log derivatives, noting that $logderiv(fg) = logderiv(f) + logderiv(g)$:

$$\frac{d}{dx}(\log f(x)) := \frac{f'(x)}{f(x)}$$

We can power series expand the log derivatives:

$$logderiv(x - x_i) = \frac{1}{x - x_i} = \frac{1}{x} + \frac{x_i}{x^2} + \frac{x_i^2}{x^3} + ...$$

So:

$$logderiv(f) = logderiv(\prod_{i=1}^{n}(x-x_i)) = \sum_{i=1}^{n} logderiv(x-x_i) = \sum_{m=0}^{\infty}\frac{1}{x^{m+1}}\sum_{i=1}^{n}x_i^m = \sum_{m=0}^{\infty}\frac{p_m(x)}{x^{m+1}}$$

where $p_m(x) := \sum_{i=1}^{n} x_i^m$. As this equals $\frac{f'}{f}$, we get that $f'(x) = f(x)(\sum_{m=0}^{\infty}\frac{p_m(x)}{x^{m+1}})$, which gives:

$$(\prod_{i=1}^{n}(x - x_i))(\sum_{m=0}^{\infty}\frac{p_m(x)}{x^{m+1}}) = nx^{n-1} - (n-1)e_1x^{n-2} + ...$$

and we can equate powers of x to get that $p_0(x) = n$, $p_1 - e_1p_0 = -(n-1)e_1$, $p_2 - e_1p_1 + e_2p_0 = (n-2)e_2$, and so on to recursively solve for p_i. This will let us express an arbitrary p_i in terms of the elementary symmetric functions. As an example of this, consider finding $\alpha^5 + \beta^5 + \gamma^5$ for the roots α, β, γ of $z^3 + z + 1$. You can use this as a reference to find the elementary symmetric polynomials in these variables: https://brilliant.org/wiki/newtons-identities/

- **Discriminants**: If the roots of a polynomial f are $\{x_1, ..., x_n\}$, we define:

$$\Delta := \prod_{i<j}(x_i - x_j)$$

Δ is an antisymmetric polynomial, so Δ^2 is symmetric. We call (some multiple of) Δ^2 the **discriminant** of f. Δ^2 vanishes iff f has multiple roots, and f has multiple roots iff f and f' have a common factor, i.e. if $Res(f, f') = 0$.

- **The Resultant**: The goal here is to determine a test to see when two polynomials have a common factor (which is equivalent to them having a common root if K is algebraically closed). Suppose $f(x) = \sum_{i=1}^{m} a_ix^i$, $g(x) = \sum_{i=0}^{n} b_ix^i$. Then we have that $f(x)p(x) + g(x)q(x) = 0$ for nonzero p, q– take $p\frac{g}{x-a}$, $q = \frac{-f}{x-a}$ where a is the root. This expression $f(x)p(x)+g(x)q(x) = 0$ is a set of linear equations (equating powers) which gives us the **Sylvester Matrix**. The determinant of this matrix is

the **resultant** of f and g, $Res(f,g)$, and this is 0 if and only if f and g have a common factor.

We know that f has a mulitple root iff its discriminant is 0, and also iff it has a common root with f'. So, we suspect that $Res(f,f')$ and Δ^2 should be proportional. In fact, if f has degree n, then we have the relation:

$$Res(f,f') = (-1)^{n(n-1)/2} a_0 Disc(f)$$

- Example: A curve $f(x_1,...,x_n)$ is **nonsingular** if all its $f(x_1,...,x_n) = 0, \frac{\partial f}{\partial x_i} = 0$ has no simultaneous solution for all i. When is $y^2 = x^3 + bx + c$ nonsingular? This happens iff $2y = 0$ and $3x^2 + b = 0$. But $y = 0 \implies x^3 + bx + c = 0$, so the curve is nonsingular if the equations:

$$x^3 + bx + c = 0 \qquad\qquad 3x^2 + b = 0$$

have no solution. This is equivalent to the resultant being nonzero, and it turns out that the resultant is $\pm(4b^3 + 27c^2)$. So, the curve is nonsingular iff $4b^3 + 27c^2 \neq 0$.
- **Graded Rings**: We say that A is a graded ring if:

$$A = \oplus_{i \in \mathbb{N}} A_i$$

where $A_i A_j \subset A_{i+j}$. For example, $\mathbb{C}[X]$ is graded by degree, as:

$$\mathbb{C}[X] = \mathbb{C} \oplus \mathbb{C}x \oplus \mathbb{C}x^2 \oplus ...$$

- **Reynold's Operators**: If R is the ring of invariants, the Reynold's operator is a map:

$$\rho : \mathbb{C}[x_1,...,x_n] \to R$$

taking

$$\rho(f) := \frac{1}{|G|} \sum_{g \in G} g \cdot f$$

which is an invariant because if we act any $g \in G$ on this, we can pull it inside the sum and reindex, as $g' \mapsto g \cdot g'$ is a bijection for finite groups. The Reynold's operator satisfies:

$$\rho(f+g) = \rho(f) + \rho(g) \qquad\qquad \rho(1) = 1$$

and if f is an invariant, then:

$$\rho(fg) = f\rho(g)$$

For example, if $G = S_n$ and $f = x_1$, then $\rho(f) = \frac{e_1}{n}$.
- **Invariant Theory**: Suppose a finite G acts on a complex vector space V with basis $\{x_1,...,x_n\}$. We wish to find the polynomials invariant under the action of G. For example, if $G = A_n$ and $V = \mathbb{C}^n$, then the ring of invariants is the ring of symmetric polynomials, and generated by $e_1,...,e_n,\Delta$. Hilbert proved that the **ring of invariants is always finitely generated over** $\mathbb{C}$. To prove this, note $\mathbb{C}[x_1,...,x_n]$ is graded. Let I be the ring of invariants. As the ring is graded:

$$I = \mathbb{C} \oplus (\oplus_{m=1}^{\infty} I_m)$$

where I_m is the set of homogenous invariant ideals of degree m. The ideal J generated by $\oplus_{m=1}^{\infty} I_m$ is finitely generated by Hilbert's Theorem, so let this ideal be generated by $i_1, ..., i_n$. We will show that these elements generate this **as a ring**, not as an ideal. Suppose these elements generate $I_1, ..., I_k$ (**TODO justify this: something about graded rings.**). Pick $f \in I_{k+1}$. Then, $f \in J$, so:

$$f = a_1 i_1 + ... + a_n i_n$$

where $a_i \in \mathbb{C}[x_1, ..., x_n]$. Each of these i_j are invariant, as is f, so applying the Reynold's operator gives:

$$\rho(f) = \rho(a_1) i_1 + ... + \rho(a_n) i_n$$

But ρ maps into the ring of invariants, so this is an $R - linear$ combination of elements that generate R, and hence $\rho(f) = f$ is in the ring generated by the $i_1, ..., i_n$, which completes the proof.

Example: Let $G = \mathbb{Z}/n\mathbb{Z}$ act on $\mathbb{C}[x, y]$, and let σ be a generator for G. Define the action by:

$$\sigma(x) := \xi x \qquad\qquad \sigma(y) := \xi y$$

where ξ is the primitive nth root of unity $exp(2\pi i/n)$. The ring of invariants is then all polynomials consisting of monomials of total degree n.

4. 10 / 26 (Power Series)

- **Formal Power Series**: We define the **formal power series ring** with coefficients in R, $R[[X]]$, as the set of formal power series $\{a_0 + a_1 x + a_2 x^2 + ... : a_i \in R\}$ with componentwise addition and polynomial multiplication. By "formal", we mean that the sum need not converge. An equivalent construction is:

$$R[[X]] := \varprojlim R[X]/(x^n)$$

We see this intuitively because we get natural projections $R[X]/(x^{n+1}) \to R[X]/(x^n)$ by projecting, and so we can reverse propagate this to get an arbitrary element of $R[[X]]$ (see my class notes). This is the **completion of R[X] at the ideal** $I = (x)$. More generally, recall that if I is an ideal, then $I^n := (\{a_0 a_1 ... a_n : a_i \in I\})$. More generally, if I is an ideal of a ring R, we define the **completion of** R **at** I to be the inverse limit $\varprojlim R/I^n$.
- **Units of** $K[[X]]$: Let $f(x) = \sum_{n=0}^{\infty} a_n x^n \in R[[X]]$. If $a_0 \neq 0$, then f has an inverse. We assume $a_0 = 1$ WLOG, and so $f(x) = 1 + g(x)$ where $g(x)$ is all the higher order terms. Then:

$$f^{-1} = (1+g)^{-1} = 1 - g + g^2 - g^3 + ... = \sum_{n=0}^{\infty} (-1)^n g^n$$

For example, take $f(x) = 1 + x + x^2$. Then:

$$f^{-1} = 1 - (x + x^2) + (x + x^2)^2 - (x + x^2)^3 + ... = 1 - x + x^3 + ...$$

- **Ideals of $K[[X]]$**: The only ideals of $K[[X]]$ are (0), (1), and (x^n) for $n \in \mathbb{N}$. This is because any element $x = \sum_{n=k}^{\infty} a_n x^n = x^k \sum_{n=0}^{\infty} a_n x^n = x^k u$ for a unit u. Thus, $K[[X]]$ **is a PID and a UFD**.
- If R is Noetherian, so is $R[[X]]$ and $R[[X_1, ..., X_n]]$.

  This proof just follows the one we did before for $R[X]$– let I be an ideal. Take I_0 to be all the coefficients on x^0 for the elements of I, I_1 to be the coeff on x^1 for elements of I with $a_0 = 0$, and so on. Then, this forms a chain, as if $\sum_{n=k}^{\infty} a_n x^n \in I$, so is $\sum_{n=k}^{\infty} a_n x^{n+1} = x \sum_{n=k}^{\infty} a_n x^n$. This chain stabilizes and is finitely generated, and these elements generate $R[[X]]$.
- **Weierstrauss Preparation**: Let $f \in K[[X, Y]]$. We may write $f = ug$, where u is a unit, and $g \in K[[X]][Y]$ is an element with leading coefficient a power of x.

  Essentially, we can "fool" a variable into thinking that f is a polynomial in the other ring. The idea is this: Take the smallest coefficient on f, i.e. pick a monomial $x^m y^n$ such that $a_{m,n} \neq 0$ and if $a < m$ or $a = m, b < n$, then $a_{a,b} = 0$. Then, we may kill off all the variables $x^m y^l$ with $l > n$ by multiplying by a unit, and similarly we may kill off the monomial terms on $x^a y^b$ with $a > m$ and $b \geq n$. This unit is well defined because any coefficient on y^n only needs a finite number of computations.
- $K[[X, Y]]$ **is a UFD**.

  The proof we gave for $R[X]$ works for any Noetherian ring, and $K[[X, Y]]$ is Noetherian. Uniqueness follows from Weierstrauss Preparation. We must show that irreducible $\implies$ prime in $K[[X, Y]]$. Suppose f is irreducible, and that $f|gh$. We may assume that $f, g, h \in K[[X]][Y]$ by Weierstrauss. $K[[X]]$ is a UFD (already shown), so $K[[X]][Y]$ is, and thus $f|g$ or $f|h$ in $K[[X]][Y]$. But this implies that $f|g$ or $f|h$ in $K[[X, Y]]$, so irreducibles are prime. Now the proof is easy to complete as if we have two different irreducible factorizations, each element must divide into each other element bijectively, so they must be unique up to associate.
- Example: In $K[X, Y]$, $y^2 - x^2 - x^3$ is irreducible. However, it is reducible in $K[[X, Y]]$, as we may write:

$$y^2 - x^2 - x^3 = (y + x\sqrt{1 + x})(y - x\sqrt{1 + x})$$

  The geometric explanation for this in $K[X, Y]$ is that the curve is a single loop and irreducible. However, in $K[[X, Y]]$, we only consider the curve where we have convergence– this is in a circle about the origin, and so we see that we have two distinct branches, which corresponds to a factorization.
- **Hansel's Lemma**: Let $f \in K[[X, Y]]$ with smallest nonzero coefficient of degree d forming a polynomial $f_d(x, y)$. Suppose $f_d(x, y) = g(x, y)h(x, y)$ with g and h coprime. Then, we may lift this factorization to $K[[X, Y]]$, i.e. $f(x, y) = G(x, y)H(x, y)$ where g and h are the smallest degree terms of G and H.

  In the following example, $f_d(x, y) = y^2 - x^2$ factorizes into a coprime product, which lifts to the power series ring. In number theory, we replace $K[[X]]$ with the p-adic integers:

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$$

Suppose $f(x) \equiv 0 \mod p$, $f \in \mathbb{Z}[X]$. If $f'(x) \not\equiv 0 \mod p$, then $f(x) = 0$ has a root in $\mathbb{Z}_p$, so $f(x) \equiv 0 \mod p^n$ has a root for all n. For example, consider $f(x) = x^2 - 7$. This has a root $1 \mod 2$ and $f'(0) \equiv 0 \mod 2$, so f has a root mod 2^n for all n.