

Something Something

Fmoc

December 29, 2024

There are something I should have learnt back in my first two years as an undergraduate.

1 Polynomials

1.1 Some Divisibility

Proposition 1.1. Let R be a UFD, $X \in R$, $a, b \in \mathbb{Z}_{\geq 1}$. Then the ideal

$$(X^a - 1) + (X^b - 1) = (X^{(a,b)-1}).$$

In particular, the gcd

$$(X^a - 1, X^b - 1) = X^{(a,b)} - 1.$$

1.2 Resultant and Discriminant

Let K be a field. We want to know when are two polynomials $f, g \in K[X]$ coprime.

Lemma 1.1. $(f, g) \neq 1 \iff \exists u, v \in K[X] \setminus \{0\}$ s.t. $\begin{cases} fu = gv, \\ \deg u < \deg g, \deg v < \deg f. \end{cases}$

Proof. If $(f, g) \neq 1$, then put $u = g/(f, g)$, $v = f/(f, g)$.

If $(f, g) = 1$ and $fu = gv$, then $u \mid g$, $v \mid f$, so $g/u = f/v$ divides $(f, g) = 1$, meaning $u = g, v = f$. \square

Now assume $fu = gv$ for some $u, v \in K[X]$ with $\deg u < \deg g, \deg v < \deg f$. Lemma 1.1 shows that, $(f, g) \neq 1$ iff $fu = gv$ has nonzero solution. This is a linear equation in the K -vector space $K \oplus KX \oplus \dots \oplus KX^{m+n-1}$, and it has a nonzero solution iff and only if the discriminant is zero.

Definition 1. Let A be a commutative ring, $f, g \in A[X]$. We define the **resultant** of $f = \sum_{i=0}^n a_i X^i$ and $g = \sum_{j=0}^m b_j X^j$ to be¹

$$\text{res}_X(f, g) := \begin{vmatrix} \left. \begin{matrix} a_n & \cdots & a_0 \\ & a_n & \cdots & a_0 \\ & & \ddots & \\ & & & a_n & \cdots & a_0 \end{matrix} \right\} m \\ \left. \begin{matrix} b_m & \cdots & b_0 \\ & b_m & \cdots & b_0 \\ & & \ddots & \\ & & & b_m & \cdots & b_0 \end{matrix} \right\} n \end{vmatrix},$$

¹Of course, we require $\deg f = n$ and $\deg g = m$.

a determinant of an $(n+m) \times (n+m)$ -matrix over A .

So we can rephrase Lemma 1.1 into: $f, g \in K[X]$ are coprime if and only if their resultant $\text{res}_X(f, g) \neq 0$.

Now assume that both f and g split in K . Then $(f, g) \neq 1 \iff f$ and g share at least one same root. This suggests that $\text{res}_X(f, g)$ should be divided by *all* $x - y$, where x is a root of f and y is a root of g ; multiplicity are considered here.

Theorem 1. If $f = \sum_{i=0}^n a_i X^i = \prod_{i=1}^n (X - x_i)$ and $g = \sum_{j=0}^m b_j X^j = \prod_{j=1}^m (X - y_j)$, are polynomials that splits in K , then

$$\text{res}_X(f, g) = a_n^m b_m^n \prod_{i=1}^n \prod_{j=1}^m (x_i - y_j).$$

In particular, we can study if a polynomial has multiple roots (in its splitting field) using resultant.

Definition 2. Let A be a commutative ring and $f(X) = a_n X^n + \dots + a_0 \in A[X]$. The **discriminant** of f is

$$\text{disc}(f) := \frac{(-1)^{\frac{1}{2}n(n-1)}}{a_n} \text{res}_X(f, f') \in A,$$

where $f'(X) = na_n X^{n-1} + \dots + a_1$ is the derivative of f .

Note that $\text{res}_X(f, f')$ is a multiple of a_n , because its first column is ${}^t(a_n \ 0 \ \dots \ 0 \ na_n \ 0 \ \dots \ 0)$, and we require $a_n \neq 0$. Thus $\text{disc}(f)$ is well-defined.

So f has multiple roots iff $\text{disc}(f) = 0$.

Example 1.1. (1) If $f(X) = aX^2 + bX + c$, then $\text{disc}(f) = -\frac{\text{res}_X(f, f')}{a} = b^2 - 4ac$.

(2) If $f(X) = X^3 + pX + q$, then $\text{disc}(f) = -\text{res}_X(f, f') = -(4p^3 + 27q^2)$.

Proposition 1.2. Let $f(X) = a_n X^n + \dots + a_0 \in K[X]$, then

$$\text{disc}(f) = a_n^{2n-2} \prod_{1 \leq i < j \leq n} (x_i - x_j)^2,$$

where x_1, \dots, x_n are all the roots of f in a fixed splitting field with multiplicity counted.

Proof. By Theorem 1,

$$\text{res}_X(f, g) = a_n^m \prod_{i=1}^n g(x_i).$$

Use this to compute. □

2 Elementary Number Theory

2.1 Valuation of Binomial Coefficients

Proposition 2.1. Let $n \in \mathbb{Z}_{\geq 1}$, then

$$\begin{aligned} v_p(n!) &= \sum_{i \geq 1} \left\lfloor \frac{n}{p^i} \right\rfloor \\ &= \frac{n - \text{sum of digits in the expansion of } n \text{ in base } p}{p - 1}. \end{aligned}$$

For example, $v_p(p^r!) = \frac{p^r - 1}{p - 1}$.

Proof. Think and you'll find the first equality trivial.

If $n = \sum_{i \geq 0} n_i p^i$ with $0 \leq n_i \leq p - 1$, then

$$\left\lfloor \frac{n}{p^i} \right\rfloor = \frac{n - (n_0 + n_1 p + \cdots + n_{i-1} p^{i-1})}{p^i}, \quad i \geq 1.$$

So

$$\begin{aligned} v_p(n!) &= n \sum_{i \geq 1} \frac{1}{p^i} - \sum_{i \geq 1} \sum_{j=0}^{i-1} n_j p^{j-i} \\ &= \frac{n}{p-1} - \sum_{j \geq 0} n_j \sum_{i \geq j+1} p^{j-i} = \frac{n - \sum_{j \geq 0} n_j}{p-1}. \end{aligned}$$

□

Corollary 2.1 (Kummer). Let $a, b \in \mathbb{Z}_{\geq 1}$, then

$$\begin{aligned} v_p \left(\binom{a+b}{b} \right) &= \sum_{i \geq 1} \left(\left\lfloor \frac{a+b}{p^i} \right\rfloor - \left\lfloor \frac{a}{p^i} \right\rfloor - \left\lfloor \frac{b}{p^i} \right\rfloor \right) \\ &= \# \text{ of carries when compute } a + b \text{ in base } p. \end{aligned}$$

Proof. Note that if $n = \sum_{i \geq 0} n_i p^i$ for $0 \leq n_i \leq p - 1$, then

$$\left\lfloor \frac{n}{p^i} \right\rfloor = \frac{n - (n_0 + n_1 p + \cdots + n_{i-1} p^{i-1})}{p^i}.$$

By definition, there is a carry at p^i in $a + b$ means that

$$(a_0 + a_1 p + \cdots + a_{i-1} p^{i-1}) + (b_0 + b_1 p + \cdots + b_{i-1} p^{i-1}) \geq p^i.$$

So Proposition 2.1 gives the result.

□

3 Commutative Algebra

3.1 Nakayama Lemma

3.2 Flatness

Recall:

$$\text{preserve } \varprojlim \iff \text{right-adjoint} \implies \text{left-exact} \iff \text{right-derivative} \iff \text{preserve } \textit{finite} \varprojlim$$

3.2.1 Definition

Let A be a commutative ring, M an A -module. We say M is **flat** over A , if the tensor-with- M functor $(-) \otimes_A M$ is exact; i.e., the tensor-with- M functor preserves injections:

$$N \hookrightarrow N' \implies N \otimes_A M \hookrightarrow N' \otimes_A M'.$$

Proposition 3.1 (Basic properties of flat modules). Let A be a commutative ring, B an A -algebra.

(a) free \implies flat.

(b) (Tensor) M flat over A & N flat over $A \implies M \otimes_A N$ flat over A .

(c) (Base change) M flat over $A \implies M \otimes_A B$ flat over B .

(d) (Transitivity) B flat over A & M flat over $B \implies M$ flat over A .

Theorem 2. An A -module M is flat if and only if for every ideal I of A , $I \otimes_A M \rightarrow IM$ is an isomorphism.

Corollary 3.1. Over a PID, flat \iff torsion-free.

3.2.2 Local Nature of Flatness

Corollary 3.2. Over a Dedekind domain, flat \iff torsion-free.

3.3 Cyclotomic Extensions

Fix an algebraic closure \bar{F} of a field F . An n -th root of unity is $\zeta \in F$ s.t. $\zeta^n = 1$. A **primitive n -th root of unity** is an n -th root of unity $\zeta \in \mu_n(\bar{F})$ s.t.

$$\zeta^d = 1 \iff n \mid d.$$

Proposition 3.2. Assume $\text{char } F \nmid n$, then:

- $\mu_n(\bar{F}) \simeq \mathbb{Z}/n\mathbb{Z}$ as group, and the generators of $\mu_n(\bar{F})$ are precisely the n -th *primitive* roots of unity.
- $F(\mu_n)$ is the splitting field of $X^n - 1$ over F , and $F(\mu_n)/F$ is Galois with an embedding

$$\chi_n : \text{Gal}(F(\mu_n)/F) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$$

defined by

$$\sigma(\zeta) = \zeta^{\chi_n(\sigma)}, \quad \forall \zeta \in \mu_n, \sigma \in \text{Gal}(F(\mu_n)/F).$$

Cyclotomic Polynomials

Definition 3. The n -th **cyclotomic polynomial** is

$$\Phi_n(X) := \prod_{d|n} (X^d - 1)^{\mu(n/d)},$$

where $\mu : \mathbb{Z}_{\geq 1} \rightarrow \{0, \pm 1\}$ is the Möbius function.

Example 3.1. If $p \in \mathbb{Z}$ is a prime, then

$$\Phi_{p^n}(X) = \frac{X^{p^n} - 1}{X^{p^{n-1}} - 1}, \quad \forall n \in \mathbb{Z}_{\geq 1}.$$

Theorem 3. The polynomial $\Phi_n(X) \in \mathbb{Z}[X]$ is monic with integral coefficients of degree $\varphi(n) = \#\mathbb{Z}/n\mathbb{Z}$. These polynomials are characterised by

$$\prod_{d|n} \Phi_d(X) = X^n - 1, \quad \forall n \geq 1.$$

In addition, $\Phi_n(X)$ is irreducible over \mathbb{Q} .

4 Schemes

In this section, all rings are assumed to be commutative.

4.1 Some Properties of Schemes

4.1.1 Reduced Schemes

A ring A is reduced if its nilradical $\text{nil}(A) = 0$.

A scheme X is said to be **reduced at** $x \in X$, if the local ring $\mathcal{O}_{X,x}$ is reduced. We say that X is **reduced** if it is reduced at every point.

Proposition 4.1. Let X be a scheme. Then TFAE:

- (a) X is reduced.
- (b) $\forall U \subset X$ open, $\mathcal{O}_X(U)$ is reduced.
- (c) \exists affine cover $\{U_i\}$ of X , s.t. all $\mathcal{O}_X(U_i)$ are reduced.

To prove this, we consider an ideal sheaf \mathcal{N}_X on X defined by

$$\mathcal{N}_X(U) := \{s \in \mathcal{O}_X(U) \mid s_x \in \text{nil}(\mathcal{O}_{X,x})\},$$

so that X is reduced $\iff \mathcal{N}_X = 0$

Proposition 4.2. Let Z be a closed subset of the scheme X . Then there is a unique structure of reduced scheme on Z , making it a closed subscheme of X .

In particular, there is a unique closed subscheme $i : X_{\text{red}} \hookrightarrow X$ with the same topological space as X . More precisely, $X_{\text{red}} = V(\mathcal{N}_X) = (X, \mathcal{O}_X/\mathcal{N}_X)$. This subscheme X_{red} verifies the following property:

- If Y is a reduced scheme, then any morphism $Y \rightarrow X$ factors through $Y \rightarrow X_{\text{red}} \rightarrow X$.

Proof of Proposition 4.1 and Proposition 4.2. Let $U \subset X$ be an affine open. Then since taking radical commutes with localization, we have $\mathcal{N}_X(U) = \text{nil}(\mathcal{O}_X(U))$. This proves Proposition 4.1. We also see that $|V(\mathcal{N}_X)| = |X|$.

Next, we verify that the closed ringed subspace $X_{\text{red}} := (X, \mathcal{O}_X/\mathcal{N}_X)$ of X is a scheme (and, of course, reduced); that is, it is locally affine. So assume $X = \text{Spec } A$. Let $N = \text{nil}(A)$ and $i : \text{Spec } A/N \rightarrow \text{Spec } A$ the closed embedding. For any $g \in A$, we know that the kernel of

$$A_g = \mathcal{O}_{\text{Spec } A}(D(g)) \rightarrow \mathcal{O}_{\text{Spec } A/N}(D(\bar{g})) = (A/N)_{\bar{g}}$$

is $N \otimes_A A_g$, which $= \text{nil}(A_g) = \mathcal{N}_X(D(g))$; i.e, $\ker i^\# = \mathcal{N}_X$. Hence $X_{\text{red}} \simeq \text{Spec } A/N$ is a scheme.

Now let Z be a closed subset of X . We first show that the reduced closed subscheme (Z, \mathcal{O}_Z) is unique if it exists. For an affine open $U \subset X$, $(Z \cap U, \mathcal{O}_Z|_{Z \cap U})$ is a closed subscheme of U , so it is isomorphic to $\text{Spec } \mathcal{O}_X(U)/I$ for some ideal $I \subset \mathcal{O}_X(U)$. As a subset of $U = \text{Spec } \mathcal{O}_X(U)$, $Z \cap U = V(I)$. Since Z is reduced, $\text{nil}(\mathcal{O}_X(U)/I) = 0$, namely I is radical. If there is another reduced closed subscheme structure of X on Z , it must also be given by a radical ideal $J \subset \mathcal{O}_X(U)$ on U , and $V(I) = V(J)$. But for radical ideals, this means $I = J$.

To make Z a reduced closed subscheme, take affine cover $\{U_i = \text{Spec } A_i\}_i$ of X and ideals $I_i \subset A_i$ s.t. $Z \cap U_i = V(I_i)$. We endow $Z \cap U_i$ with the reduced scheme structure of $\text{Spec } A_i/\sqrt{I_i}$ and use uniqueness to glue them. \square

4.2 Irreducible Components

A topological space X is **irreducible** if it is *not* the union of proper closed subsets.

- The closure of a irreducible subset is irreducible.
- The set of irreducible subsets in a space X admits maximal w.r.t. inclusions, called **irreducible components**.

4.3 Integral Schemes

A scheme X is said to be **integral at** $x \in X$, if the local ring $\mathcal{O}_{X,x}$ is an integral domain.

4.4 Normal Schemes

An integral domain A is normal if it is integrally closed in its fraction field.

4.5 Regular Schemes

A scheme X is said to be **normal at** $x \in X$, if the local ring $\mathcal{O}_{X,x}$ is (an integral domain and) normal.

5 Some Properties of Morphisms

5.1 Seperated Morphisms

5.2 Quasi-Compact Morphisms

A morphism $f : X \rightarrow Y$ of schemes is said to be **quasi-compact**, if the inverse image $f^{-1}(V)$ of any affine open $V \subset Y$ is quasi-compact.

Proposition 5.1. Let $f : X \rightarrow Y$ be a morphism of schemes.

- (1) If f is a closed immersion, then f is quasi-compact.
- (2) If f is an open immersion, and Y is locally Noetherian, then f is quasi-compact.

5.3 Morphisms of Finite Type

A ring homomorphism $A \rightarrow B$ is of finite type if it make B a finitely generated A -algebra.

A morphism $f : X \rightarrow Y$ of schemes is said to be **of finite type**, if

- f is quasi-compact, and
- For any affine open $V \subset Y$ and affine open $U \subset f^{-1}(V)$, the map $\mathcal{O}_Y(V) \rightarrow \mathcal{O}_X(f^{-1}(V)) \rightarrow \mathcal{O}_X(U)$ is of finite type.

5.4 Proper Morphisms

5.5 Flat Morphisms

A morphism $f : X \rightarrow Y$ of schemes is said to be **flat at** $x \in X$, if $f_x^\# : \mathcal{O}_{Y,f(x)} \rightarrow \mathcal{O}_{X,x}$ is flat. We say that f is **flat** if it is flat at every point.

5.6 Unramified Morphisms

5.7 Étale Morphism

5.8 Smooth Morphisms