Something Something

Fmoc

November 20, 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

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

In particular, the gcd

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

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 $K \oplus KX \oplus \cdots \oplus KX^{m+n-1}$, 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 be[1]

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

[1] Of 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 $\operatorname{res}_X(f,g) \neq 0$.

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 $\operatorname{res}_X(f,g)$ 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 $f=\sum_{i=0}^n a_iX^i=\prod_{i=1}^n(X-x_i)$ and $g=\sum_{j=0}^m b_jX^j=\prod_{j=1}^m(X-y_j)$, are polynomials that splits in K, then

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

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 $f(X)=a_nX^n+\cdots+a_0\in A[X]$. The **discriminant** of f is

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

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

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

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

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

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

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

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

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

Proof. By Theorem 1,

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

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

$$v_p(n!)=\sum_{i\geq 1}\left\lfloor\frac{n}{p^i}\right\rfloor.$$

Proof. Think and you'll find it trivial. □

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

.

$$v_p\left(\binom{a+b}{b}\right) = \sum_{i\geq 1}\left(\left\lfloor\frac{a+b}{p^i}\right\rfloor - \left\lfloor\frac{a}{p^i}\right\rfloor - \left\lfloor\frac{b}{p^i}\right\rfloor\right). \qquad \square$$

Corollary 2.2 (Kummer)**.** Expand $a, b \in \mathbb{Z}_{\geq 1}$ in base p, then

$$v_p\left(\binom{a+b}{b}\right) = \#\text{ of carries when compute } a+b \text{ in base } p.$$

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. $\square$

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, $I \otimes_A M \to IM$ 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 $\operatorname{char} F \nmid n$, then:

- $\mu_n(\bar{F}) \simeq \mathbb{Z}/n\mathbb{Z}$ as group, and the generatos of $\mu_n(\bar{F})$ are precisely the n-th *premitive* 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

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

  defined by

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

Cyclotomic Polynomials

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

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

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

Example 2. 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

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

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