

7.2. Rank

an $n \times n$ -matrix

Prnk The rank of M is the largest $0 \leq r \leq n$ s.t. some $r \times r$ -minor of M (made from r not necessarily consecutive rows and columns) has nonzero determinant.

Cor 7.2.1 $\text{rk}(M) \geq \text{rk}(M \bmod p) \quad \forall \text{ prime } p$

with equality if p doesn't divide ~~any~~ the (nonzero) det of a ^{particular} $r \times r$ -minor of M , where $r = \text{rk}(M)$.

Cor 7.2.2

$\text{rk}(M) = \max_{p \in \mathbb{N}} \text{rk}(M \bmod p)$ if $\prod_{p \in \mathbb{N}} p \mid \det(M)$

$\rightarrow T(M) := \prod_{p \in \mathbb{N}} p \mid \det(M)$
 $(\sum_{i=1}^n m_{ii})^{1/2}$ (2 B. any mins)

which can be computed in time

$$O((n + \log \|\det(M)\|) \cdot \frac{2}{3} n^\omega) \dots$$

Prnk If $\prod_{p \in \mathbb{N}} p \nmid \det(M)$ and $N' \geq N$, then the probability

that a random prime $p \leq N'$ doesn't satisfy

$$\text{rk}(M) = \text{rk}(M \bmod p)$$

$$\text{is at most } \frac{\#\{p \leq N\}}{\#\{p \leq N'\}}.$$

~~This~~ This gives rise to a Monte Carlo alg. with

$$\text{running time } O(n^\omega + \underbrace{(u + \log \|\det(M)\|) \cdot \log \log (u + \log \|\det(M)\|)}_{\text{time to find primes } p < u + \log \|\det(M)\|})$$

time to find ~~primes~~
 primes $p < u + \log \|\det(M)\|$

7.3. Resultants

Prop Let $f, g \in \mathbb{Z}[X]$ be ~~pol.~~ ^{monic pol.} ~~relatively prime in $\mathbb{Z}[X]$~~

~~which~~ If $f, g \pmod{p}$ are relatively prime in $\mathbb{F}_p[X]$, then f, g are rel. prime in $\mathbb{Z}[X]$.

The converse doesn't hold:

~~Ex. X^2+1 is prim. in $\mathbb{Z}[X]$, but $X^2+1 = (X+1)^2 \pmod{2}$.~~

~~Could there be many such~~

~~Ex~~

E.g. $X^2+1, X+1$ are rel. prime in $\mathbb{Z}[X]$, but $X^2+1 = (X+1)^2 \pmod{2}$

Q If f, g are rel. prime over \mathbb{Q} , for which p are they not rel. prime ~~in~~ \pmod{p} ?

Def For any $d \geq 0$, let $K[X]_{\leq d} := \{f \in K[X] : \deg(f) \leq d\}$.

Lemma 7.3.1 Let $f, g \in K[X]$ be ~~pol.~~ ^{pol.} of degrees n, m .

Then, ~~gcd~~ $\gcd(f, g) = 1$ if and only if

the map $\begin{matrix} \{a \in K[X] : \deg(a) \leq m\} \times \{b \in K[X] : \deg(b) \leq n\} \\ (a, b) \end{matrix} \xrightarrow{K[X]_{\leq m+n}} \{c \in K[X] : \deg(c) \leq m+n\} \rightarrow f a + g b$

is an isomorphism.

Prf Note that $\dim(\text{LHS}) = m+n = \dim(\text{RHS})$.

" \Leftarrow " If $\gcd(f, g) = c$ ~~is not constant~~, then the image only contains multiples of $\gcd(f, g)$. \Rightarrow The map isn't surjective.

" \Rightarrow " The map is an isom. according to ~~Bezout's identity~~ Bezout's identity. \square

Def The resultant $\text{Res}(f,g)$ of ~~pol.~~ pol. $f, g \in K[x]$ of deg. u, m is the determinant of the map in Lemma 7.3.1 w.r.t the basis $(1, 0, (x, 0), \dots, (x^{m-1}, 0), (0, 1), \dots, (0, x^{u-1}))$ of the LHS and the basis $(1, x, \dots, x^{u+m-1})$ of the RHS.

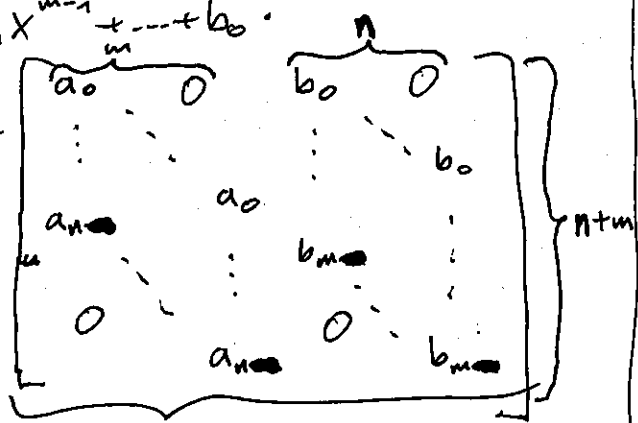
Cor 7.3.2 $\text{gcd}(f, g) = 1 \Leftrightarrow \text{Res}(f, g) \neq 0$.

Cor 7.3.3 Let $f, g \in \mathbb{Q}[x]$ be pol. and let p be a prime not dividing the denominator of any coeff. of f or g . Then, f, g are rel. prime mod p iff $p \nmid \text{Res}(f, g)$.

Example Let

$$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 \text{ and } g(x) = x^m + b_{m-1}x^{m-1} + \dots + b_0.$$

show $\text{Res}(f, g) = \det$



Sylvester matrix

Lemma 7.3.3

a) $\text{Res}(g, f) = (-1)^{nm} \text{Res}(f, g)$

c) $\text{Res}(f, g) = a_n^m b_m^n \cdot \prod_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} (\alpha_i - \beta_j) = a_n^m \prod_{1 \leq j \leq m} g(\alpha_i)$

if $\alpha_1, \dots, \alpha_n \in \bar{K}$ are the roots of f (with mult.)
and $\beta_1, \dots, \beta_m \in \bar{K}$

b) $\text{Res}(r f, s g) = r^m s^n \text{Res}(f, g) \quad \forall r, s \in K^*$

Of a), b) clear

c) w.l.o.g. f and g are monic: $a_n = b_m = 1$.

$\Rightarrow f(x) = \prod_i (x - \alpha_i), \quad g(x) = \prod_j (x - \beta_j)$

\Rightarrow coeff. a_k of f is hom. pol. in $\alpha_1, \dots, \alpha_n$ of deg $n-k$.

-- b_l of g -- -- β_1, \dots, β_m -- -- $m-l$.

$\Rightarrow \text{Res}(f, g)$ is hom. pol. in $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m$ of deg. nm .

Expand the determinant

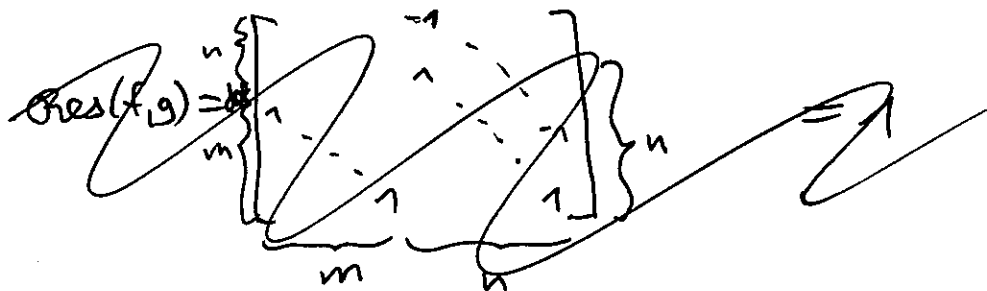
~~if $(\alpha_i)_i \in \bar{K}^n, (\beta_j)_j \in \bar{K}^m$ satisfy $\alpha_i = \beta_j$ for some i, j , then $X - \alpha_i \mid f, g$, so $\text{gcd}(f, g) \neq 1$, so $\text{Res}(f, g) = 0$~~

$\Rightarrow \prod_{i,j} (\alpha_i - \beta_j) \stackrel{\text{divides}}{\sim} \text{Res}(f, g)$ as a pol. in $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m$
deg. nm

$\Rightarrow \text{Res}(f, g) = C_{nm} \cdot \prod_{i,j} (\alpha_i - \beta_j)$ for some constant C_{nm}

To show $C_{n,m} = 1$, it suffices to check the equality for one pair (f, g) of pol. f, g of deg. n, m .

For example, look at $f(x) = x^n$, $g(x) = x^m + 1$



$$\alpha_1 = \dots = \alpha_n = 0, \beta_j$$

$$\text{Res}(f, g) = \det \begin{bmatrix} \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \end{bmatrix} = 1$$

$$\alpha_1 = \dots = \alpha_n = 0$$

$$\Rightarrow \prod_{i,j} (\alpha_i - \beta_j) = \left(\prod_j (1 - \beta_j) \right)^n = 1.$$

const. coeff.
of g

□

Prmk Resultants can be computed using the ^(fast) Euclidean algorithm. (HW)

over fields K
with $\mathcal{O}(1)$
arithmetic

~~•~~ • The CRT trick then allows us to compute resultants of polynomials in $\mathbb{Q}[X]$, in part. to determine whether two pol. in $\mathbb{Q}[X]$ are relatively prime.