7.2. Rank

Rmk The rank of an $n\times n$-matrix M is the largest $0\le r\le n$ 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 $\mathrm{rk}(M) \ge \mathrm{rk}(M \bmod p) \quad \forall \text{ primes } p$

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

Cor 7.2.2 $\mathrm{rk}(M) = \max\limits_{p\le N} \mathrm{rk}(M \bmod p)$ if $\prod\limits_{p\le N} p > T(M) := \prod\limits_i \max\left(1, \left(\sum\limits_j m_{ij}^2\right)^{1/2}\right)$ (≥ B(any mino

which can be computed in time

$O((n+\log T(M))\cdot n^{\omega})$ ...

Rmk If $\prod\limits_{p\le N} p > T(M)$ and $N'\ge N$, then the probability that a random prime $p\le N'$ doesn't satisfy

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

is at most $\dfrac{\#\{p\le N\}}{\#\{p\le N'\}}$.

This gives rise to a Monte Carlo alg. with running time $O\Big(n^{\omega} + \underbrace{(n+\log T(M))\cdot\log\log(n+\log T(M))}_{\text{time to find primes } p \ll n+\log T(M)}\Big)$

7.3. Resultants

Rmk Let $f, g \in \mathbb{Z}[X]$ be monic pol. ~~relatively prime in $\mathbb{Q}[X]$~~ If $f, g \bmod p$ are relatively prime in $\mathbb{F}_p[X]$, then f, g are rel. prime in $\mathbb{Q}[X]$.

The converse doesn't hold:

~~E.g. X^2+1 is irred. in $\mathbb{Q}[X]$, but $X^2+1=(X+1)^2 \bmod 2$.~~

~~Could there be so many bad~~

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

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

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

Lemma 7.3.1 Let $f, g \in K[X]$ be pol. of degrees n, m. Then, $\gcd(f,g)=1$ if and only if the map

$$\overset{K[X]_{<m}}{\cancel{\{a \in K[X] : \deg(a)<m\}}} \times \overset{K[X]_{<n}}{\cancel{\{b \in K[X] : \deg(b)<n\}}} \to \overset{K[X]_{<n+m}}{\cancel{\{c \in K[X] : \deg(c)<n+m\}}}$$

$$(a \quad , \quad b) \mapsto fa+gb$$

is an isomorphism.

Pf Note that $\dim(LHS) = m+n = \dim(RHS)$.

$K[X]_{<m} \cong K[X]/f$, $K[X]_{<n} \cong K[X]/g$, $K[X]_{<n+m} \cong K[X]/fg$.

"$\Leftarrow$" ~~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 Bézout's identity. □

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

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

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 $p \nmid \mathrm{Res}(f,g)$.

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

Then $\mathrm{Res}(f,g) = \det$

$$\underbrace{\left(\begin{array}{cccccc} \multicolumn{3}{c}{\overbrace{\qquad\qquad\quad}^{m}} & \multicolumn{3}{c}{\overbrace{\qquad\qquad\quad}^{n}} \\ a_0 & & 0 & b_0 & & 0 \\ \vdots & \ddots & & \vdots & \ddots & b_0 \\ & & a_0 & & & \vdots \\ a_n & & \vdots & b_m & & \vdots \\ & \ddots & & 0 & \ddots & \vdots \\ 0 & & a_n & & & b_m \end{array}\right)}_{\text{Sylvester matrix}} \left.\vphantom{\begin{array}{c} a\\a\\a\\a\\a\\a \end{array}}\right\} n+m$$

Lemma 7.3.3

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

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

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

b) $\mathrm{Res}(rf, sg) = r^m s^n\, \mathrm{Res}(f,g) \quad \forall r,s \in K^\times$

Pf 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 --- $\beta_1,\dots,\beta_m$ --- $m-l$.

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

Expand the determinant

If $(\alpha_i)_i \in \overline{K}^n$, $(\beta_j)_j \in \overline{K}^m$ satisfy $\alpha_i = \beta_j$ for some i, j, then $X-\alpha_i \mid f, g$, so $\gcd(f,g) \ne 1$, so Res(f,g)=

$$\Longrightarrow \underbrace{\prod_{i,j} (\alpha_i - \beta_j)}_{\deg nm} \overset{\text{divides}}{\mid} \underbrace{\mathrm{Res}(f,g)}_{\deg.\, nm} \text{ as a pol. in } \alpha_1,\dots,\alpha_n,\beta_1,\dots,\beta_n$$

$\Longrightarrow \mathrm{Res}(f,g) = C_{n,m} \cdot \prod_{i,j} (\alpha_i - \beta_j)$ for some constant $C_{n,}$

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 $f(x)=x^n$, $g(x)=x^m+1$

~~$\mathrm{Res}(f,g)=\begin{array}{c}n\{\\m\{\end{array}\underbrace{\begin{bmatrix} & & 1 & & \\ & & 1 & \ddots & \\ 1 & & & \ddots & 1 \\ & \ddots & & & \\ & & 1 & & 1\end{bmatrix}}_{m \quad n}\}n = 1$~~

~~$\alpha_1 = \dots = \alpha_n = 0$, β~~

$$\mathrm{Res}(f,g) = \det\begin{bmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & 1 & \\ 1 & & \vdots & & \ddots \\ & \ddots & 1 & & 1\end{bmatrix} = 1$$

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

$$\Rightarrow \prod_{i,j}(\alpha_i-\beta_j) = \Big(\underbrace{\prod_j(-\beta_j)}_{\text{const. coeff. of } g}\Big)^n = 1.$$

□

Rmk 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 $\mathbb{Z}[X]$, in part. to determine whether two pol. in $\mathbb{Q}[X]$ are relatively prime.