Math 501: Problem Session 2

Clear that \((x-y)/(\sum_{i=2}^k x_i y_i^{k-i}) \equiv x^{k+1} - y^{k+1} \text{ in } \mathbb{Z}[x,y].\)

Idea: "universal property": for any ring \(R\), any \(a, b \in R\) have a unique ring hom \(\phi: \mathbb{Z}[x,y] \to R\) s.t. \(\phi(x), \phi(y) = a, b\) \(\Rightarrow\) an identity in \(\mathbb{Z}[x,y]\) is an identity in any ring.

Here, in any ring \(S,\ x-a \mid x^k - a^k \text{ in } R = S[x].\)

(In general, \(x_1, \ldots, x_r\) in \(\mathbb{Z}[x_1, \ldots, x_r]\) are "r generic elements"

for any ring)

By induction, if \(R(x) = (x-a_0) \cdots (x-a_r)\)
\(P,Q \in R[x],\ a_1, \ldots, a_r \in R,\ \text{and } P(a_{k+1}) = 0 \text{ but } a_{k+1} \neq a_k \text{ for } (i \leq k)\)
then \(Q(a_{k+1}) = 0 \text{ so } Q = (x-a_{k+1})^T, T \in R[x].\)
and \(P = (x-a_1) \cdots (x-a_{k+1})^T\)
if \(R\) is an integral domain

But if \(ab = 0\) in \(R,\) but \(a, b \neq 0\) then \(P(x) = ax\) has genus \(b > 0,\) but \((x-a) (x-b) \neq P\) (any multiple of \(x(x-1)\)
has degree \(\geq 2).\)

Rational root test: Suppose \(x = \alpha\) is a root of \(f \in \mathbb{Z}[x]\)
write: \(f = \sum_{k=0}^n a_k x^k.\) Multiply by \(\alpha^k,\) plug in \(\alpha.\) Get:
\[ \sum_{k=0}^{n} \alpha_k \beta^{n-k} = 0 \]

(5) Reduce mod \( b \), get \( \alpha_n \cdot \beta^0 = 0 \). \( \beta \) is invertible \( \Rightarrow \) \( \alpha_n = 0 \). \( \Rightarrow \) \( b | \alpha_n \).

Reduce mod \( a \), get \( \alpha_0 \beta^n = 0 \). (a)

If \( a \) is non-zero get \( a | \alpha_0 \). (if \( a = 0 \) get \( \alpha_0 = 0 \))

Points: reduces checking if \( f \) has rational roots to a finite search.

Example: \( \sigma(b) \). If \( t^4 + 1 \) has a rational root then the root is in \( \mathbb{Z} \) (polynomial is monic).

(Def: Call an algebraic number \( \alpha \) an algebraic integer if \( \alpha \) is a root of a monic polynomial \( f \in \mathbb{Z}[x] \).

and \( f(x) = 0 \) for some monic \( f \in \mathbb{Z}[x] \).

and the root divides 1, but \((\pm) t^4 + 1 \neq 0 \)

(or: \( t^4 + 1 = 0 \) for all \( t \in \mathbb{R} \), so no real roots even.)

(in general: If \( f \) can be factored over \( \mathbb{R} \), \( f \) can be factored over any extension ring \( S \).) (If \( f \) can be factored over \( \mathbb{R} \), it's can be factored over quotient rings.)

Consider \( \sigma(a) \), \( \sigma(b) \). Need to factor \( t^4 + 1 \) over \( \mathbb{Q} \), over \( \mathbb{R} \).

Since no roots, any factorization is into quadratic factors. Over any field, we want \( \sigma \) \( \sigma \) if

\[ t^4 + 1 = (t^2 + at + b)^2 (t^2 - at + \frac{1}{b}) \]

forced by \( \frac{1}{b} \) \( \sigma \) coeff of \( t^2 \)

forced by constant coeff.
(in principle should have gotten 5 eqns in 6 unknowns, but why can assume monic factors, use constraints set 2 eqns in two unknowns:)

\[ \text{coeff of } t^2 : b + \frac{1}{b} - a^2 = 0 \]

\[ \text{coeff of } t : \frac{1}{b} - ab = 0 \]

\[ a(5 - 1) \]

either \( a = 0 \), \( b + \frac{1}{b} = 0 \), so \( b^2 = -1 \).

(in a field having \( b \) st. \( b^2 = -1 \), \( (t^2 + b)(t^2 - b) = t^4 + 1 \).

(doesn't exist in \( \mathbb{R} \), hence in \( \mathbb{Q} \) )

so \( a \to \frac{1}{b} = b \), i.e. \( b = \pm 1 \), \( a^2 = \pm 2 \).

in both \( \mathbb{R}, \mathbb{Q} \) can't have \( a^2 = -2 \), so \( a^2 = 2 \).

in \( \mathbb{R} \), have \( (t^2 + \sqrt{2} + 1)(t^2 - \sqrt{2} + 1) = t^4 + 1 \).

in \( \mathbb{Q} \), \( t^4 + 1 \) is irreducible.

**Different solution:** Note that \( (t^2 + \sqrt{2} + 1)(t^2 - \sqrt{2} + 1) = t^4 + 1 \).

since \((\sqrt{2})^2 - 4 = -2 < 0\), both are indivisible in \( \mathbb{R}[x], \mathbb{Q}[x] \).

so this is the factorization in \( \mathbb{R}[x] \).

Suppose that \( t^4 + 1 = f \cdot g \) in \( \mathbb{Q}[x] \). Then, by unique factorization in \( \mathbb{R}[x] \), \( f, g \) are products of complementar subsets of the factors over \( \mathbb{R} \).

so here the only possible factorization is the given one, but \( \sqrt{2} \notin \mathbb{Q} \), and \( t^4 + 1 \) is irreducible in \( \mathbb{Q}[x] \).

**Example:** To factor \( t^2 + 15t^2 + 7 \) mod 3, note that
$t^4 + 15t^3 + 7 \equiv t^4 + 1 \mod 3 \quad (\text{use } (t^4 + 15t^3 + (-1)(7^2 - 5^2 + 1))$ \\
$t^4 + 15t^3 + 7 \equiv t^4 + 2 \mod 5$.

**Problem 2:** The Vandermonde Determinant.

**Philosophy:** If we have an identity
$$\det \begin{pmatrix} x_0^n & \cdots & x_0^1 \\ \vdots & \ddots & \vdots \\ x_n^n & \cdots & x_n^1 \end{pmatrix} = \prod_{i<j}(x_i - x_j)$$
in $\mathbb{Z}[x_0, \ldots, x_n]$, we can then evaluate by mapping $x_i \mapsto a_i$, over $R$, to evaluate
$$\det \begin{pmatrix} a_0^n & \cdots & a_0^1 \\ \vdots & \ddots & \vdots \\ a_n^n & \cdots & a_n^1 \end{pmatrix} \in R,$$ where $a_i \in R$.

We can use special properties of $\mathbb{Z}$, $\mathbb{Z}[x_0, \ldots, x_n]$ to get something in any ring $\mathbb{Q}(x_0, \ldots, x_n)$.

Vague argument: if $x_i = x_j$ then $V(x_0, \ldots, x_{n-1}) = 0$.

So $x_i - x_j \mid V$ true for all $i < j$, so $\prod_{i<j}(x_i - x_j) \mid V$

total degree of LHS is $(n^2)$ total degree of $V$ is $0 + n + n - 1 = \frac{n^2}{2}$

So ratio is a constant $c \in \mathbb{Z}$.

**Make this formal:**

1. Consider $V(x_0, \ldots, x_{n-1})$ as a polynomial in $x_{n-1}$
   with coeffs in $\mathbb{Z}[x_0, \ldots, x_{n-2}]$. Then this poly has deg $n-1$
   in $x_{n-1}$. It has $x_0, \ldots, x_{n-2}$ as zeroes (the determinant
   $V(x_0, \ldots, x_{n-2}, x_1)$ vanishes if $i \leq n-2$ since it has good roots.)
So by Problem 1(c),
\[ V(x_0, \ldots, x_{n-1}) = \prod_{i \neq j} (x_i - x_j)V_{n-2}(x_0, \ldots, x_{n-2}) \]
with \( V_{n-2}(x_0, \ldots, x_{n-2}) \in \mathbb{Z}[x_0, \ldots, x_{n-2}] \) ("polynomial of degree 0 in \( \mathbb{Z}[x_0, \ldots, x_{n-2}] \)).

Some argument shows \( \prod_{i \neq j} (x_i - x_j) \) divides \( V \) for any \( j \).

\( V_{n-2} \) has degree \( n-2 \) in each of \( x_0, \ldots, \) \( x_{n-2} \).

It has the roots \( x_0, \ldots, x_{n-2} \) (co-poly in \( \mathbb{Z}[x_0, \ldots, x_{n-2}] \)[\( x_{n-2} \)])

because plugging \( x_j \) (\( 0 \leq j \leq n-2 \)) into \( x_{n-2} \), we get:

\[ 0 = V(x_0, \ldots, x_{n-2}, x_j, x_{n-2}) = \prod_{i=0}^{n-2} (x_i - x_{n-1}) (x_j - x_{n-1}) \cdot V(x_0, \ldots, x_{n-2}, x_j) \]

so \( V = \prod_{0 \leq i < j \leq n-1} (x_i - x_j) \cdot V_{n-2}(x_0, \ldots, x_{n-2}) \text{ integral domain } \mathbb{Z}[x_0, \ldots, x_{n-1}] \)

Continue by induction.

End: \( V = \prod_{0 \leq i < j \leq n-1} (x_j - x_i) \cdot V_1 \), \( V_1 \in \mathbb{Z} \).

To find \( V_1 \), consider monomial \( \prod x_i^{a_i} \).

To set it, choose \( x_{n-1} \) for each factor \( (x_{n-1} - x_i) \)

(there are \( 2^n \) choices when applying distributive law to

\( \text{from } x_{n-1} - x_{n-2} \text{ already choose } x_{n-1} \))
Every monomial \( \prod_{i=0}^{n-1} x_i \) occurs in \( \det(\mathbf{A}) \) with coeff 1, \( \text{sgn} (\text{id}) = 1 \).

So \( V_{-1} = 1 \).

\[
\det (A) = \sum (-1)^{\pi} \prod_{i=0}^{n-1} x_i
\]

\( \det (a \ b) = ad - bc \)

\( \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc \)

One mathematical object can have many definitions, constructions. Useful to look at all of them.

Example \( \mathbb{Q}(\sqrt{2}) \):

1. Intersection of all subfields of \( \mathbb{R} \) (or \( \mathbb{C} \)) that contain \( \sqrt{2} \).
2. All elements of \( \mathbb{R} \) of the form \( a + b\sqrt{2} \).
3. Elements of \( \mathbb{Q} \) obtained from \( a + b\sqrt{2} \) by arithmetic operations.

\( \mathbb{R} = (1) \) complete ordered field

(2) order completion of \( \mathbb{Q} \) ("Dedekind cuts")

(3) metric completion of \( \mathbb{Q} \) ("Cauchy sequences")
Aside: determinants

Let $V$ be a $n$-dim vector field $F$.

Def: A function $f: V^d \to F$ is

1. $k$-linear if it's linear in every variable $x_i$:
   \[ f(x_1, x_2, \ldots, x_k) = \alpha f(x_1, \ldots, x_k) + f(x_1, x_2, \ldots) \]

   [eq. $x_1$ is $3$-linear $F^3 \to F$]

2. Alternating if $f(x_1, \ldots, x_k) = 0$ whenever $x_i = x_j$ for some $i \neq j$.

   Exs: if $T \in SL$ is a transposition then
   \[ f(x_1, \ldots, x_k) = -f(x_1, \ldots, x_k) \]
   converse also if $1 \neq 1$.

   Ideal: if $f(x, x) = 0$ then $f(x+y, x+y) = f(x, x) + f(y, y) + f(y, y) + f(x, x)$

   If $f(x, x) + f(x, x) = \Delta (1+1) = f(x, y) + f(y, x)$

3. Volume form if it's $n$-linear & alternating ($n = \dim V$)

Cor of ex: if $f$ is alternating, $0 \in S_n$ then $f(x_1, \ldots, x_k) = \delta_{i}^{(n)} f(x_1, \ldots, x_k)$.

Def: write $V^\wedge n$ for the space of volume forms on $V$.

Ex: $V^\wedge n$ is a subspace of the space of functions on $V$.\]
Fix basis $\beta_i; \beta_1, \ldots, \beta_n \in V$.

Prop: The map $V^n \to F$ given by

$$\Phi: \beta_i \mapsto \phi_i$$

is injective.

Proof: Let $\nu_i; \nu_1, \ldots, \nu_n$ be vectors. Need to show: $\phi_i(\nu_1, \ldots, \nu_n)$ determined by $\nu_i$ and by $\phi_i(\beta_1, \ldots, \beta_n)$

$\Rightarrow$ have any $\nu_i = \sum_j a_{ij} \beta_j$

$\Rightarrow$ $\phi_i(\nu_1, \ldots, \nu_n) = \phi_i(\sum_j a_{ij} \beta_j, \ldots, \sum_j a_{ij} \beta_j)$

$= \sum_j \sum_{i=1}^n (a_{ij}, a_{ij}, \ldots, a_{ij}) \cdot \phi_i(\beta_j, \ldots, \beta_j)$

Due to linearity,

$$= \sum_{\sigma: \Sigma i = \Sigma j} \prod_{i=1}^n a_{ij} \sigma(i) \cdot \phi_i(\beta_{\sigma(i)}, \ldots, \beta_{\sigma(n)})$$

Note: if $\sigma$ is not injective then $\phi_i(\beta_{\sigma(i)}, \ldots, \beta_{\sigma(n)}) = 0$

$\Rightarrow$

$$= \sum_{\sigma: \Sigma i, \sigma(i)} \prod_{i=1}^n a_{ij} \sigma(i) \phi(\beta_{\sigma(i)}, \ldots, \beta_{\sigma(n)}) = \left( \sum_{\sigma: \Sigma i, \sigma(i)} \prod_{i=1}^n a_{ij} \sigma(i) \right) \phi_i(\beta_1, \ldots, \beta_n)$$

Only depends on $a_{ij}$

$\Rightarrow \phi_i(\nu_1, \ldots, \nu_n)$

$\Rightarrow \dim F(V^n) \leq 1$

Best $\phi(\nu_1, \ldots, \nu_n) = \sum_{i=1}^n a_{ij} \Phi_i(\beta_j)$ if $\nu_i = \sum_j a_{ij} \beta_j$.
is a volume form (cf. from Lin ch 1)
\[ \Phi(b_1, \ldots, b_n) = 1 \to \]
so \( \dim F V = 1 \) (Lemma)
Define: let \( \tau : V \to V \) be a linear map
the map \( V \to V \)
\[ \varphi \to \varphi \circ \tau \]
is linear, so for scalar \( \alpha \) and \( \beta \)
\[ \varphi(Tv_1, \ldots, Tv_n) = (\det \alpha) \cdot \varphi(v_1, \ldots, v_n) \]
for all \( v_1, \ldots, v_n \).
(Check to check: \( (\alpha \varphi + \beta \varphi)(Tv_1, \ldots, Tv_n) = \]
\[ = \alpha \varphi(Tv_1, \ldots, Tv_n) + \beta \varphi(Tv_1, \ldots, Tv_n) \]
and \( \varphi(Tv_1, \ldots, Tv_n) \) is a volume form)

**Observe:**
\[ \varphi(TSv_1, \ldots, TSv_n) = \varphi(S, \ldots, S) \]
\[ = \varphi(S, \ldots, S) \cdot \varphi(v_1, \ldots, v_n) \]
\[ = (\det S) \cdot (\det T) \cdot (\det S) \]
\[ = (\det T) \cdot (\det S) \]
check if \( T \) has matrix \( A = (a_{ij}) \) at basis \( \{e_i\} \)?
then \( \det T = \sum_{i,j,k} (e_i, e_j, e_k) \)
if \( i \neq j \neq k \)

**Recall:** let \( \varphi \) be \( T \)