THE ALGEBRA OF FORGETFULNESS

Matt Baker, Georgia Tech

Upstate NY Number Theory Colloquium

December 2020

OUR FIRST PROTAGONIST

René Descartes

DESCARTES' RULE OF SIGNS

Let $P(x) = a_0 + a_1 x + \cdots + a_n x^n$ be a polynomial with real coefficients.

Descartes' Rule: The number of **positive** real roots of P(x) is at most the number of **sign changes** in the sequence of coefficients $a_0, a_1, \ldots, a_n$.

It follows (replacing x by -x) that the number of **negative** real roots of P(x) is at most the number of sign changes in the sequence $a_0, -a_1, \ldots, (-1)^n a_n$

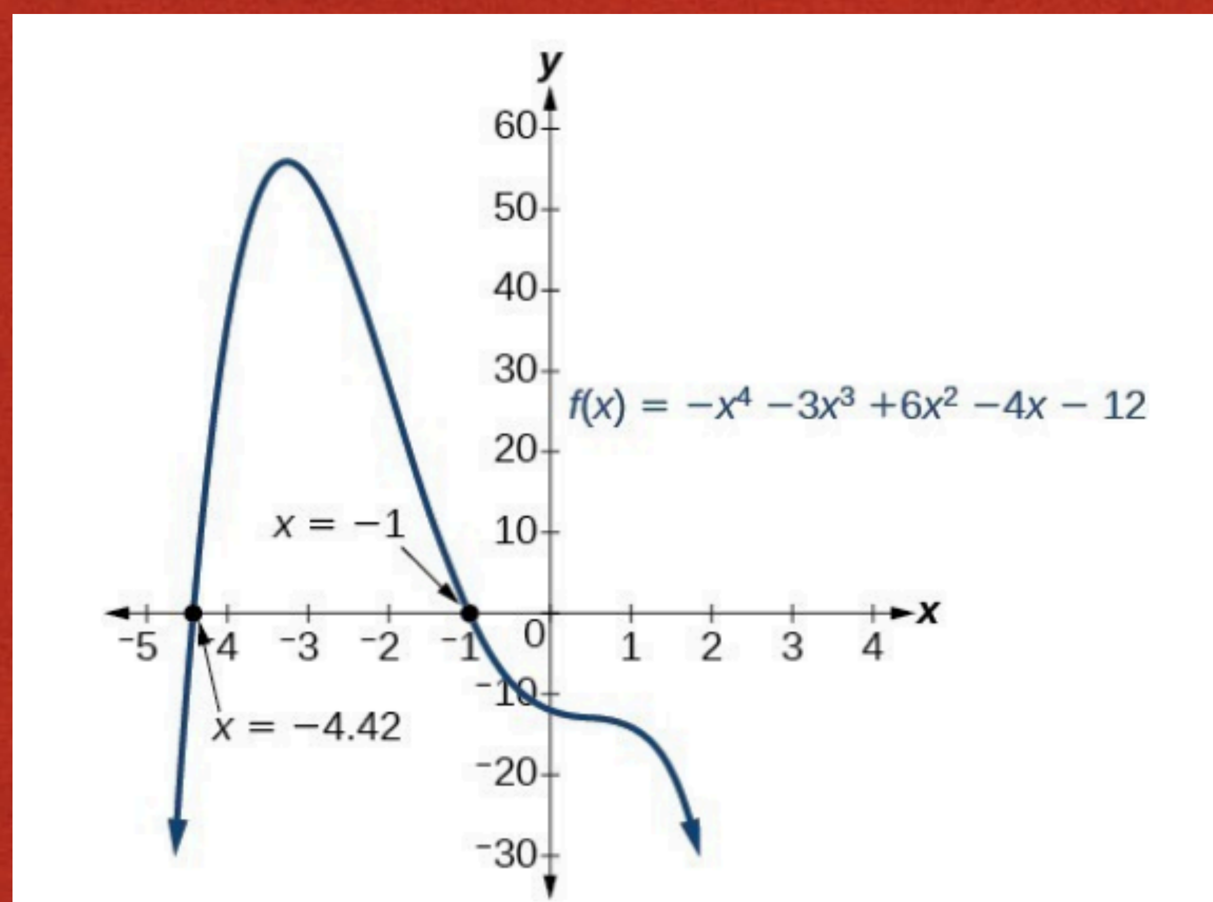
SUPPLEMENT TO THE RULE

Although we won't focus on this aspect of Descartes' rule, it's worth mentioning that the difference between the number of positive roots and the number of sign changes is in fact always EVEN.

AN EXAMPLE

$$f(x) = -x^4 - 3x^3 + 6x^2 - 4x - 12$$

$$f(-x) = -x^4 + 3x^3 + 6x^2 + 4x - 12$$



OUR SECOND PROTAGONIST

VALUATIONS

Let K be a field.

A valuation on K is a map $v : K \to \mathbb{R} \cup \infty$ such that:

$$v(x) = 0 \Leftrightarrow x = 0$$
$$v(xy) = v(x) + v(y)$$
$$v(x+y) \geq \min\{v(x), v(y)\}$$

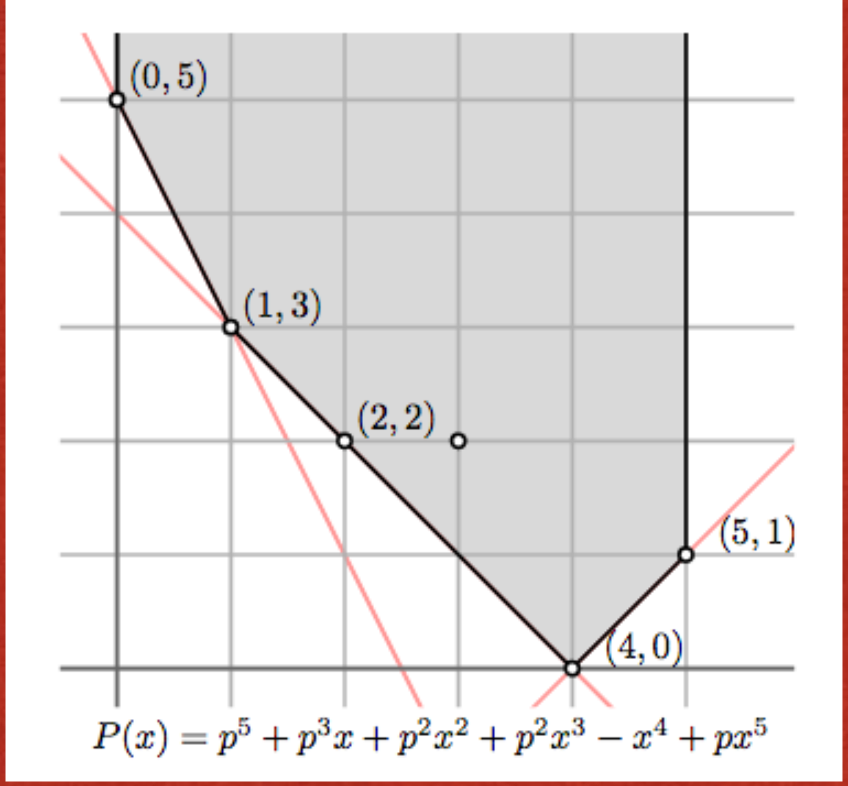
EXAMPLES OF VALUATIONS

- The order of vanishing of a Laurent series f(T) at T=0
- The p-adic valuation of a rational number (for some prime p), e.g.

$$v_5(17/125) = v_5(17) - v_5(125) = 0 - 3 = -3$$

THE NEWTON POLYGON

The **Newton polygon** of $P(x)=a_0+a_1x+...+a_nx^n$ with coefficients in a field K equipped with a valuation is the lower convex hull of the points $(i,v(a_i))$.



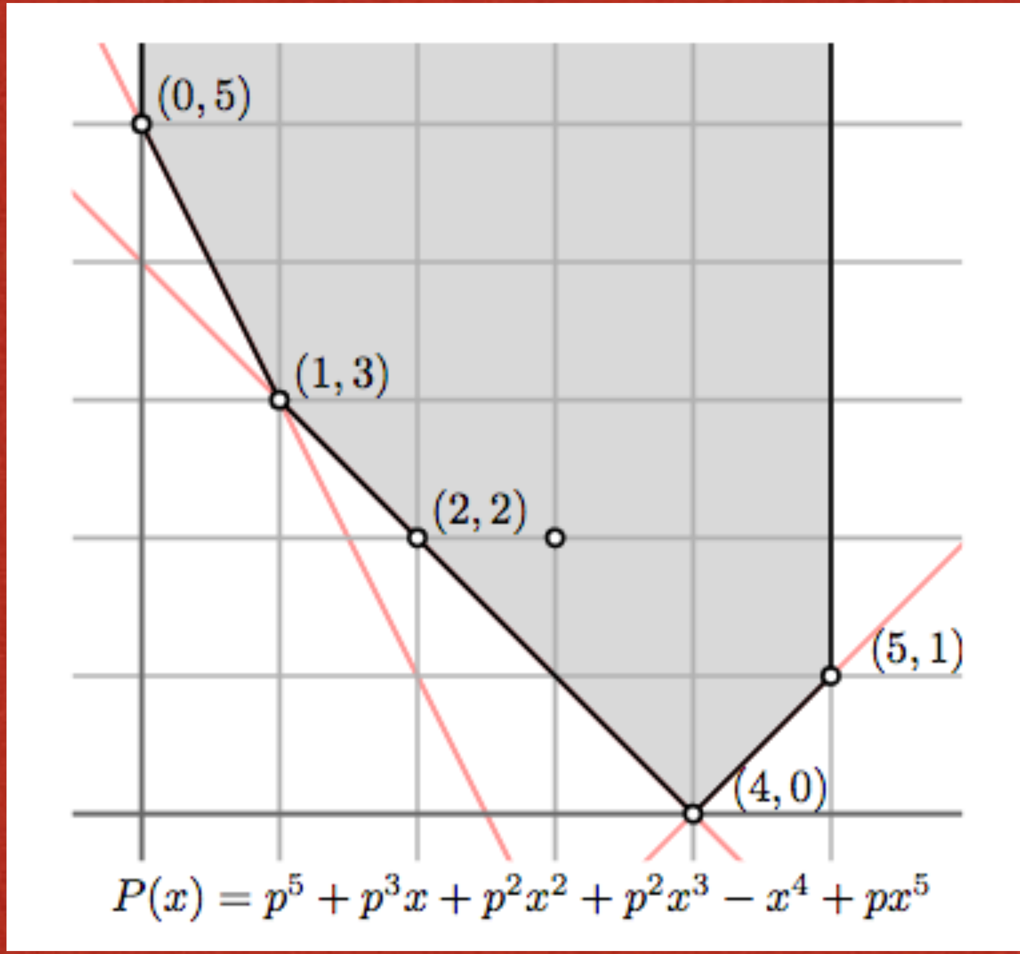
$$\text{slopes} : -2, -1, +1$$
$$\text{multiplicities} : 1, \quad 3, \quad 1$$

NEWTON'S POLYGON RULE

Let $P(x)=a_0+a_1x+...+a_nx^n$ be a polynomial with coefficients in a field K equipped with a valuation v.

<u>Newton's Polygon Rule</u>: The number of roots of P(x) in K with valuation equal to s is at most the multiplicity of -s in the Newton polygon of P.

REVISITING OUR EXAMPLE



$$\text{minus slopes} : 2, \quad 1, -1$$

$$\text{multiplicities} : 1, \quad 3, \quad 1$$

OUR THIRD PROTAGONIST

HYPERFIELDS

- Roughly speaking, a **hyperfield** is an algebraic structure similar to a field, but where addition is allowed to be multi-valued.
- Hyperfields were introduced by Marc Krasner in the mid-1950's.
- Like fields, hyperfields come equipped with a multiplicative identity element 1, an additive identity element 0, and a negation map $x \mapsto -x$

HYPERFIELDS (CON'T)

- However, one does not require that the hypersum of x and -x is **equal** to zero, only that zero is **contained** in the hypersum $x \boxplus -x$
- There seems to be a reappraisal of sorts going on in the math community of the "bias" against multi-valued operations.

OLEG VIRO ON MULTIVALUED OPERATIONS

"Krasner, Marshall, Connes and Consani and the author came to hyperfields for different reasons, motivated by different mathematical problems, but we came to the same conclusion: the hyperrings and hyperfields are great, very useful and very underdeveloped in the mathematical literature… Probably, the main obstacle for hyperfields to become a mainstream notion is that a multivalued operation does not fit to the tradition of set-theoretic terminology, which forces to avoid multivalued maps at any cost. I believe the taboo on multivalued maps has no real ground, and eventually will be removed. Hyperfields are legitimate algebraic objects related in many ways to the classical core of mathematics…"

THE KRASNER HYPERFIELD

$\mathbb{K} = \{0, 1\}$ with the usual multiplication and the following hyperaddition rules:

$$0 \boxplus 0 = \{0\}$$

$$0 \boxplus 1 = 1 \boxplus 0 = \{1\}$$

$$1 \boxplus 1 = \{0, 1\}$$

THE SIGN HYPERFIELD

$\mathbb{S} = \{0, 1, -1\}$ with the usual multiplication and the following hyperaddition rules:

$$0 \boxplus x = \{x\}$$
$$1 \boxplus 1 = \{1\}$$
$$-1 \boxplus -1 = \{-1\}$$
$$1 \boxplus -1 = \{-1, 0, 1\}$$

THE TROPICAL HYPERFIELD

$\mathbb{T} = \mathbb{R} \cup \{+\infty\}$ with the following rules:

$$a \odot b = a + b$$

$$a \boxplus b = \min\{a, b\} \quad \text{if} \quad a \neq b$$

$$a \boxplus b = \{c \ : \ c \geq a\} \quad \text{if} \quad a = b$$

HOMOMORPHISMS

A map $\phi : K \to F$ between hyperfields is called a **homomorphism** if:

$$\begin{aligned}
&\phi(0) = 0 \\
&\phi(1) = 1 \\
&\phi(xy) = \phi(x)\phi(y) \\
&\phi(x \boxplus y) \subseteq \phi(x) \boxplus \phi(y)
\end{aligned}$$

EXAMPLES OF HOMOMORPHISMS

- If F is a hyperfield, the map $\phi : F \to \mathbb{K}$ with $\phi(0) = 0$ and $\phi(x) = 1 \text{ for } x \neq 0$ is a homomorphism. ("Forget everything except whether x is zero or non-zero.")
- The map $\mathrm{sign} : \mathbb{R} \to \mathbb{S}$ is a homomorphism. ("Forget everything except the sign of x.")
- If K is a field and v is a valuation on K, $v : K \to \mathbb{T}$ is a homomorphism. ("Forget everything except the valuation of x.")

QUOTIENTS OF FIELDS

Here is a very general construction: let K be a field and let G be a subgroup of the multiplicative group of K. Then $K/G = (K^\times/G) \cup \{0\}$ is naturally a hyperfield.

Examples: $\mathbb{K} = \mathbb{R}/\mathbb{R}^\times$

$\mathbb{S} = \mathbb{R}/\mathbb{R}_{>0}$

POLYNOMIALS OVER HYPERFIELDS

Let F be a hyperfield. A **polynomial** with coefficients in F is a formal expression of the form

$$P(x) = a_0 + a_1 x + \cdots + a_n x^n$$

with all $a_i \in F.$

ROOTS OF POLYNOMIALS

We say that $\alpha \in F$ is a **root** of the polynomial P(x) over F if:

$$0 \in a_0 \boxplus a_1\alpha \boxplus \cdots \boxplus a_n\alpha^n$$

EXAMPLES

- When F is the sign hyperfield, 1 is a root of a nonzero polynomial P(x) iff some $a_i = 1$ and some $a_j = -1$.
- When F is the tropical hyperfield, s is a root of a nonzero polynomial P(x) iff $\min(a_i s^i)$ is achieved at least twice.

DIVISION THEOREM

We say $x - \alpha$ divides $P(x) = a_0 + a_1 x + \cdots + a_n x^n$

if there exists $Q(x) = b_0 + b_1 x + \cdots + b_{n-1} x^{n-1}$

such that $P(x) \in (x - \alpha) Q(x)$

i.e. $a_i \in (-\alpha b_i) \boxplus b_{i-1} \text{ for } i = 0, \ldots, n$

Thm: $\alpha \in F$ is a root of P(x) iff $x - \alpha$ divides P(x).

MULTIPLICITIES OF ROOTS

If α is not a root of P(x), we set $\mathrm{mult}_\alpha(P) = 0$

Otherwise, we define

$$\mathrm{mult}_\alpha(P) = 1 + \max\{\mathrm{mult}_\alpha(Q) \ : \ P \in (x-\alpha)Q\}$$

THE MULTIPLICITY INEQUALITY

Theorem (B-Lorscheid): Let $\phi : K \to F$ be a homomorphism from a field K to a hyperfield F and let P(x) be a polynomial with coefficients in K. Then for every $\beta \in F$ we have

$$\mathrm{mult}_\beta(\phi(P)) \geq \sum_{\alpha \in \phi^{-1}(\beta)} \mathrm{mult}_\alpha(P)$$

MULTIPLICITIES OVER $\mathbb{S}$

When $F = \mathbb{S}$ we show that $\mathrm{mult}_1(P)$ is equal to the number of sign changes in the coefficients of P(x).

This, together with the multiplicity inequality (applied to the homomorphism $\mathrm{sign} : \mathbb{R} \to \mathbb{S}$) implies Descartes Rule of Signs.

MULTIPLICITIES OVER $\mathbb{T}$

When $F = \mathbb{T}$ we show that $\mathrm{mult}_s(P)$ is equal to the multiplicity of $-s$ in the Newton Polygon of P(x).

This, together with the multiplicity inequality (applied to the homomorphism $v : K \to \mathbb{T}$), implies Newton's Polygon Rule.

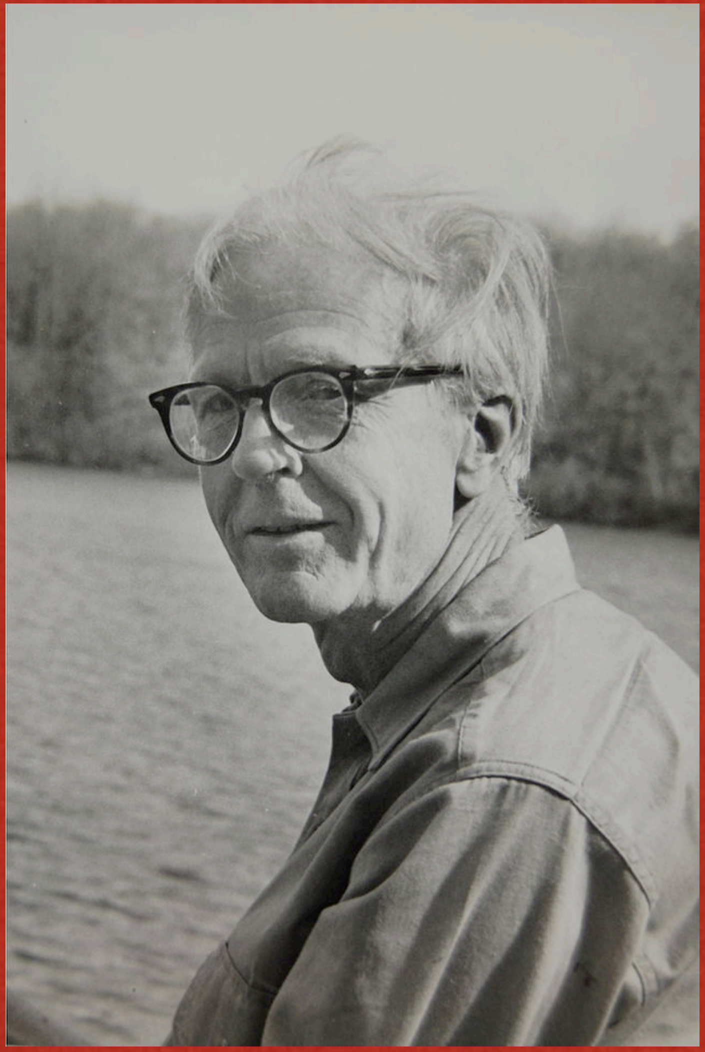
MULTIVARIATE MULTIPLICITIES

It is straightforward to generalize the notion of roots to multivariate polynomials in several variables over a hyperfield F.

Open problem: Can we generalize the notion of **multiplicities** of roots to the case of n polynomials in n variables (or, more generally, to "zero-dimensional ideals")?

Motivation: Multivariate Descartes' Rule of Signs

OUR NEXT PROTAGONISTS



Hassler Whitney

Takeo Nakasawa

MATROIDS

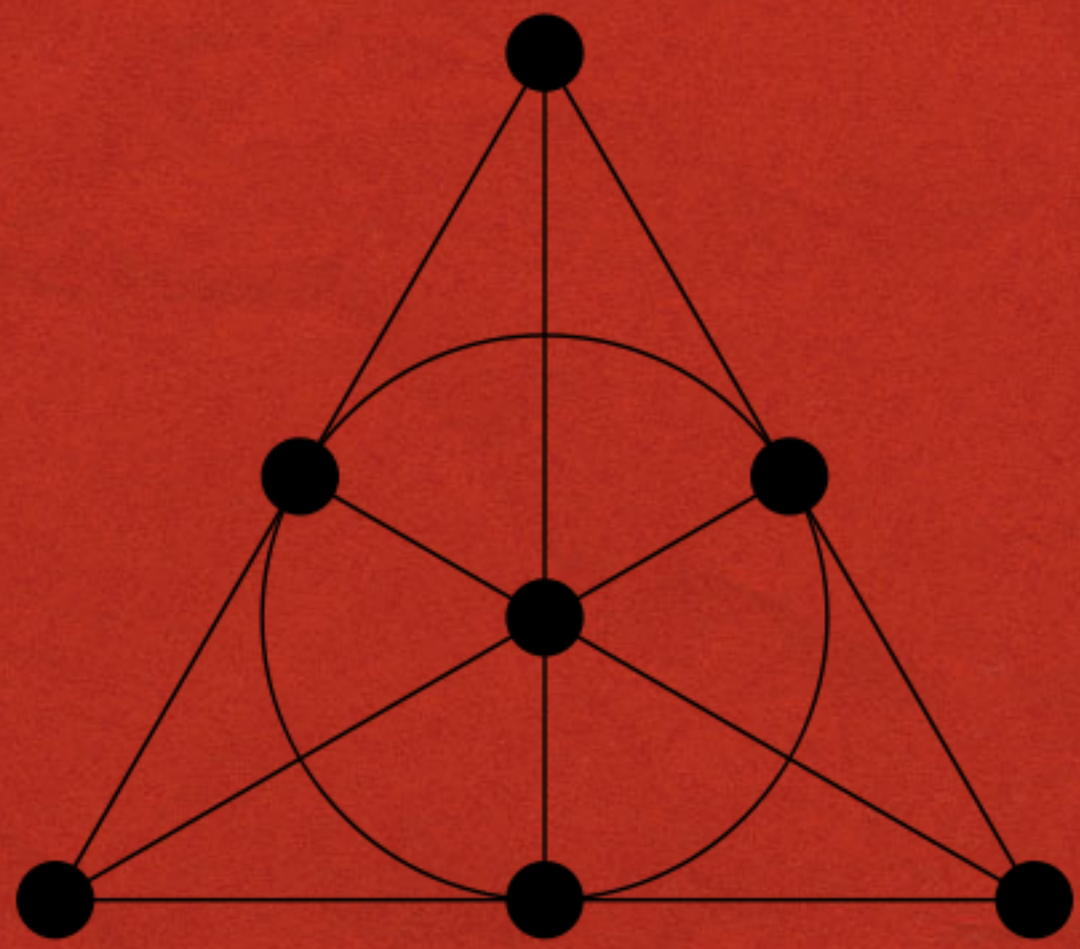
A matroid M is a finite set E together with a non-empty collection $\mathcal{B}$ of subsets of E, called the **bases** of M, such that for every $B, B' \in \mathcal{B}$ and $b \in B - B'$ there exists $b' \in B' - B$ such that $B \cup b' - b \in \mathcal{B}$

The rank of M is the cardinality of any basis B.

GIAN-CARLO ROTA ON MATROIDS

"Like many another great idea, matroid theory was invented by one of the great American pioneers, Hassler Whitney. His paper, which is still today the best entry to the subject, flagrantly reveals the unique peculiarity of this field, namely, the exceptional variety of cryptomorphic definitions for a matroid, embarrassingly unrelated to each other and exhibiting wholly different mathematical pedigrees. It is as if one were to condense all trends of present day mathematics onto a single finite structure, a feat that anyone would *a priori* deem impossible, were it not for the fact that matroids do exist."

THE FANO MATROID



GRASSMANNIANS

Let K be a field. If W is a 2-dimensional subspace of the four-dimensional vector space K^4, we can represent W as the row space of a 2x4 matrix A with entries in K.

Let a_{ij} be the determinant of the 2x2 submatrix given by the i^{th} and j^{th} columns of A.

These quantities satisfy the **Plücker equation**

$$x_{12}x_{34} - x_{13}x_{24} + x_{14}x_{23} = 0$$

GRASSMANNIANS (CON'T)

Moreover, as a point of projective space $\mathbb{P}^5_K$ the vector $(a_{12} : a_{13} : a_{14} : a_{23} : a_{24} : a_{34})$ does not depend on the choice of the matrix A, and is thus an invariant of the subspace W.

Additionally, any point of the projective space $\mathbb{P}^5_K$ satisfying the Plucker relation corresponds uniquely to a 2-dimensional subspace W.

GRASSMANNIANS (CON'T)

More generally, one can parametrize the r-dimensional subspaces of the n-dimensional vector space K^n by the points of a projective algebraic variety $\mathbb{G}(r, n)$, called the **Grassmannian**, defined by a set of equations called the **Plücker relations**.

PLÜCKER RELATIONS

In general, the Plücker relations are as follows. Let

$$I = \{x_{i_1}, \ldots, x_{i_{r-1}}\}, J = \{y_{j_1}, \ldots, y_{j_{r+1}}\}$$

with $i_1 < \cdots < i_{r-1}, j_1 < \cdots < j_{r+1}.$

Then we have

$$\sum_{k=1}^{r+1} (-1)^k x_{i_1 i_2 \cdots j_k \cdots i_{r-1}} x_{j_1 j_2 \cdots \hat{j}_k \cdots j_{r-1}} = 0.$$

THE PLÜCKER EQUATIONS OVER A HYPERFIELD

If F is a hyperfield, we can look at solutions in $\mathbb{P}_F^{\binom{n}{r}}$

to the Plücker "equations"

$$0 \in \boxplus_{k=1}^{r+1} (-1)^k x_{i_1 i_2 \cdots j_k \cdots i_{r-1}} x_{j_1 j_2 \cdots \hat{j}_k \cdots j_{r-1}}.$$

Theorem: When $F = \mathbb{K}$ is the Krasner hyperfi eld, there is a canonical one-to-one correspondence between solutions to the Plücker equations in $\mathbb{P}_{\mathbb{K}}^{\binom{n}{r}}$ and matroids of rank r on E={1,...,n}.

OTHER SOLUTIONS TO THE PLÜCKER EQUATIONS

- When F is the hyperfield of signs, solutions to the Plücker equations are the same thing as oriented matroids.
- When F is the tropical hyperfield, solutions to the Plücker equations are the same thing as tropical linear spaces (or valuated matroids).