1. Fields

Fields and vector spaces.

Typical vector spaces: $\mathbb{R}, \mathbb{Q}, \mathbb{C}$. For infinite dimensional vector spaces, see notes by Karen Smith. Important to consider a field as a vector space over a sub-field.

Also have: algebraic closure of $\mathbb{Q}$. Galois fields: $GF(p^a)$.

Don't limit what field you work over.

2. Polynomial rings over a field

Notation for a polynomial ring: $\mathbb{K}[x_1, \ldots, x_n]$.
Monomial: $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$
Set $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$.
Write x^α for $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$.
A *term* is a monomial multiplied by a field element: $c_\alpha x^\alpha$.
A *polynomial* is a *finite* $\mathbb{K}$-linear combination of monomials:

$$f = \sum_\alpha c_\alpha x^\alpha,$$

so a polynomial is a finite sum of terms. The *support* of f are the monomials that appear (with non-zero coefficients) in the polynomial f.

If $\alpha = (\alpha_1, \ldots, \alpha_n)$, put $|\alpha| = \alpha_1 + \cdots + \alpha_n$.

If $f \in \mathbb{K}[x_1, \ldots, x_n]$, $\deg(f) = \max\{|\alpha| : x^\alpha \text{ is in the support of } f\}$.

Example 2.1. $f = 7x^3y^2z + 11xyz^2$ $\deg(f) = \max\{6, 4\} = 6$. $7x^3y^2z$ is a *term*. x^3y^2z is a *monomial*.

Given $f \in \mathbb{K}[x_1, \ldots, x_n]$, *evaluation* is the map $F_f : \mathbb{K}^n \to \mathbb{K}$ given by $(c_1, \ldots, c_n) \to f(c_1, \ldots, c_n)$.

When is F_f the zero map?

Example 2.2. If $\mathbb{K}$ is a finite field, F_f can be the zero map without f being the zero polynomial. For instance take the field with two elements, $\mathbb{K} = \mathbb{Z}/2\mathbb{Z}$, and consider the polynomial $f = x^2 + x = x(x+1)$. Then f is *not* zero in the ring $\mathbb{K}[x]$, however $f(c) = 0$ for all $c \in \mathbb{K}$ (there are only two to check!).

Theorem 2.3. *If $\mathbb{K}$ is an infinite field, then F_f is the zero map if and only if f is the zero polynomial.*

Proof. (From Cox-Little-O'Shea) by induction.

If $n = 1$, then a non-zero $f \in \mathbb{K}[x]$ of degree d has at most d distinct roots (Euclidean algorithm). $F_f : \mathbb{K} \to \mathbb{K}$ evaluates to zero only at roots of f.

Assume this is true up to $n-1$ variables. Consider $\mathbb{K}[x_1, \ldots, x_n]$ as the polynomial ring $\mathbb{K}[x_1, \ldots, x_{n-1}][x_n]$ (the polynomial ring in the variable x_n with coefficients in the polynomial ring $\mathbb{K}[x_1, \ldots, x_{n-1}]$). Let $f = \sum g_i x_n^i$, where $g_i \in \mathbb{K}[x_1, \ldots, x_{n-1}]$. Consider $(\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{K}^{n-1}$. Evaluate $f(\alpha_1, \ldots, \alpha_{n-1}, x_n)$; this is a polynomial in a single variable, so by the base case it is zero if and only if $g_i(\alpha_1, \cdots, \alpha_{n-1}) = 0$ for every coefficient. By induction, $g_i(\alpha_1, \ldots, \alpha_{n-1}) = 0$ for all $(\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{K}^{n-1}$ if and only if g_i is the zero polynomial. Hence f must be the zero polynomial. □

Corollary 2.4. *Let $\mathbb{K}$ be an infinite field. Let $f, g \in \mathbb{K}[x_1, \ldots, x_n]$. Then $F_f = F_g$ if and only if $f = g$ as polynomials.*

3. Affine Varieties

Definition 3.1. Let $f_1, \ldots, f_r \in \mathbb{K}[x_1, \ldots, x_n]$. The *affine variety* cut out by $f_1, \ldots, f_r$ is denoted by $V(f_1, \ldots, f_r)$ and is defined by

$$V(f_1, \ldots, f_r) = \{c = (c_1, \ldots, c_n) \in \mathbb{K}^n : f_i(c) = 0 \text{ for all } f_1, \ldots, f_r\}$$

Example 3.2. $f = x^2 + y^2 - 1 \in \mathbb{R}[x, y]$. Then $V(f)$ = unit circle. $g = x^2 + y^2 \in \mathbb{R}[x, y]$. Then $V(g)$ = point $(0, 0)$. $h = x^2 + y^2 + 1 \in \mathbb{R}[x, y]$. Then $V(h) = \emptyset$! Notice that the codimension of these affine varieties is $1, 0, -1$, respectively.

Example 3.3. Let $f_1, f_2 \in \mathbb{R}[x, y, z]$, with $f_1 = x+y+z+7$, $f_2 = x+3y+2z+11$. Then $V(f_1, f_2)$ is a line in $\mathbb{R}^3$.

Example 3.4. Consider $f = x^2+2xy+y+1 \in \mathbb{F}_3[x, y]$. Then $V(f)$ is a *hypersurface* in $\mathbb{F}_3^3$. There are nine points in $\mathbb{F}_3^3$. If $x = 0$, $f(0, y) = y + 1$, so $y = 2$. If $x = 1$, $f(1, y) = 2$, so there are no solutions. If $x = 2$, then $f(2, y) = 2 + 2y$, so $y = 2$ again. So $V(f) = \{(0, 2), (2, 2)\}$.

Remark 3.5. Given $f_1, \ldots, f_r \in \mathbb{Z}[x_1, \ldots, x_n]$, it is interesting to consider the cardinality of $V(f_1, \ldots, f_r)$ when $f_1, \ldots, f_r$ are considered to be in finite fields of the form $GF(p^t)$. These cardinalities could be encoded in a power series, for instance. There are many open problems considering the relationships between the varieties $V(f_1, \ldots, f_r)$ over finite fields and the varieties these polynomials define over $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, etc.

Remark 3.6. Chebatorev's density theorem gives probabilistic information about the Galois group of a polynomial by looking at splitting types of the polynomial over different finite fields.

Example 3.7 (Chebatorev's density theorem in action)**.** The table below lists the orders and cycle types of transitive subgroups of the symmetric group S_4. These are the possible Galois groups of irreducible polynomials of degree four.

G	1,1,1,1	1,1,2	1,3	4	2,2	$\lvert G\rvert$
V_4	1	0	0	0	3	4
C_4	1	0	0	2	1	4
D_4	1	2	0	2	3	8
A_4	1	0	8	0	3	12
S_4	1	6	8	6	3	24

Suppose you would like to compute the Galois group of the irreducible polynomial $f(x) = x^4 + 3x^2 - 1$. Compute its factorization modulo different primes. The factorizations have to match the cycle types.

Reducing $f(x)$ modulo first 10,000 primes. Factorization type 2,2 appears 3762 times. Factorization type 1,1,1,1 appears 1222 times. Factorization type 1,1,2 appears 2514 times. Irreducible appears 2502 times.

Chebatorev's density theorem says that, in the limit, the probability that $f(x)$ factors as a particular type is precisely the probability of picking that cycle type in the Galois group.

The statistics above match the expected cycle types of the D_4 group, which is exactly what the Galois group of $f(x)$ is.

Example 3.8 (Four-bar Linkage)**.** Consider two fixed points with two rigid bars attached, and one more rigid bar connecting the movable endpoints of the two

movable bars. Attach a rigid triangle to the last bar. The curve traced out by the tip of the triangle is called the *coupler* curve of the mechanism.

Kempe's universality theorem says that any connected component of a real algebraic curve in the plane can be realized as the *coupler curve* of a mechanism. Some corrections and extensions of Kempe's theorem appear in Timothy Abbott's masters thesis. Here are some questions related to linkages:

- How can you construct a linkage with prescribed properties?
- Given a linkage, how do you find equations defining its motion?

Example 3.9 (Conformation space of cyclo-octane)**.** In cyclo-octane there are eight carbon atoms linked in a cycle by edges of a fixed length and with fixed *bond angles* between the edges at each atom. To eliminate some degrees of freedom, fix the plane determined by three atoms. So consider that three (occuring in order) have coordinates $(0,0,0)$, $(a,0,0)$, and $(b,c,0)$ (these coordinates will be completely determined by the length of the edges and the common angle). Once these are fixed, the two adjacent points on either end can each trace out a circle's worth of positions, and for each pair of choices made for the positions of these two, there are finitely many possible positions for the remaining three points. Thus the conformation space of cyclo-octane is a surface that is a finite covering of the torus $S^1 \times S^1$, and it naturally lives in $\mathbb{R}^{15}$ (the fifteen parameters come from the coordinates of the remaining 5 points which are not fixed).

Theorem 3.10. *Let $A = V(f_1, \ldots, f_r), B = V(g_1, \ldots, g_s)$, with $f_1, \ldots, f_r, g_1, \ldots, g_s \in \mathbb{K}[x_1, \ldots, x_n]$. Then $A \cup B$ and $A \cap B$ are affine varieties.*

Proof. Check that $A \cap B = V(f_1, \ldots, f_r, g_1, \ldots, g_s)$ and $A \cup B = V(\{f_i g_j : 1 \leq i \leq r, 1 \leq j \leq s\})$. □

Some questions:

- Is $V(f_1, \ldots, f_r) = \emptyset$?
- If $|V(f_1, \ldots, f_r)| < \infty$, can we find them? Can we count how many there are?
- In general, can we describe $V(f_1, \ldots, f_r)$?

4. Parametrizations of Affine Varieties

Example 4.1. Consider the variety $V(x + y + z - 3, x + 2y + 3z - 5) \subset \mathbb{R}^3$. This is defined *implicitly* (this means the variety is given by equations). Finding a Gröbner basis is a generalization of Gaussian elimination (it's Gaussian elimination on steroids). One the augmented matrix for this linear system is put in row reduced echelon form, we obtain the system

$$\begin{array}{rrl} x & -z & = 1 \\ y & -2z & = 2 \end{array}$$

From this we obtain $x = z + 1, y = -2z + 2$. Setting $z = t$, we get the *parametrization*:

$$\begin{array}{rl} x = & t + 1 \\ y = & -2t + 2 \\ z = & t \end{array}$$

Rational parametrizations

Example 4.2. Consider $V(x^2+y^2-1)$ (the unit circle). A *rational parametrization* is:

$$x = \frac{1-t^2}{1+t^2}$$
$$y = \frac{2t}{1+t^2}$$

This parametrization can be determined by considering where the line with slope t through the point $(-1,0)$ intersects the unit circle.

Definition 4.3. A *rational function* in the variables $t_1,\ldots,t_n$ is a quotient $\frac{f}{g}$ where $f,g \in \mathbb{K}[t_1,\ldots,t_n]$. Rational functions can be identified by the usual rule $\frac{f}{g} = \frac{f'}{g'}$ if and only if $fg' = f'g$. The set of all rational functions in $t_1,\ldots,t_n$ is denoted $\mathbb{K}(t_1,\ldots,t_n)$.

Proposition 4.4. *$\mathbb{K}(t_1,\ldots,t_n)$ is a field.*