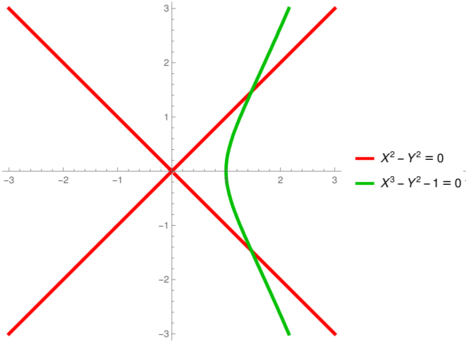
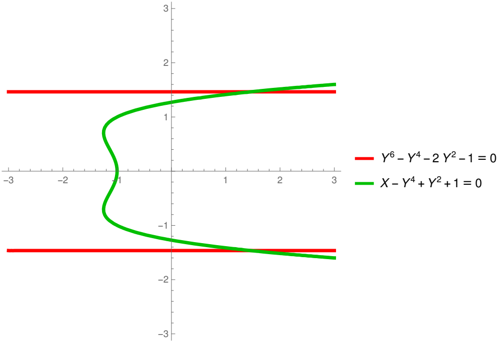
What are...Gröbner bases?

Or: Minimal intersections

The same intersection set in two different ways





Question. How can we algebraically see that the intersections match?

$$(X^2 - Y^2, X^3 - Y^2 - 1) \stackrel{?}{=} (Y^6 - Y^4 - 2Y^2 - 1, X - Y^4 + Y^2 + 1)$$

Lexicographical ordering:

$$
\begin{aligned}
f =\ & XY^3Z^5 + X^2Y^6 + X^4YZ + Y^2Z^5 + YZ^4 + Y^3 + Z^3 + XY + XZ + Z^2 + Z \\
=\ & X^4(YZ) \\
& + X^2(Y^6) \\
& + X^1\begin{pmatrix} Y^3(Z^5) \\ + Y^1(1) \\ + Y^0(Z) \end{pmatrix} \\
& + X^0\begin{pmatrix} Y^3(1) \\ + Y^2(Z^5) \\ + Y^1(Z^4) \\ + Y^0\begin{pmatrix} Z^3(1) \\ + Z^2(1) \\ + Z^1(1) \end{pmatrix} \end{pmatrix}
\end{aligned}
$$

Buchberger's algorithm

Data: Ideal $H = (h_1, ..., h_s)$
Result: Gröbner basis $G = (g_1, ..., g_t)$
init $G = H$, $G' = \emptyset$;
while $G \neq G'$ **do**
    $G' = G$;
    for $p, q \in G'$, $p \neq q$ **do**
        $s = red(S(p, q), G)$;
        if $s \neq 0$ **then**
            $G = G' \cup \{s\}$;
        end
    end
end

- $LT(p)$ = leading terms with respect to $<$ My fixed ordering (important!)
- lcm = least common multiple
- $S(p, q) = \frac{\mathrm{lcm}(LT(p), LT(q))}{LT(p)} p - \frac{\mathrm{lcm}(LT(p), LT(q))}{LT(q)} q$
- $red(S(p, q), G)$ reduce $S(p, q)$ mod G

Enter, the theorem

A generating set $G = (g_1, ..., g_t)$ of an ideal I is a Gröbner basis if:

for any $p \in I \setminus \{0\}$ there exists g_i such that $LT(g_i)|p$

G is reduced if the coefficients of $LT(g_i)$ is 1 and no monomial of the g_i is in the ideal generated by $LT(g_j)$ for $i \neq j$

(a) Buchberger's algorithm constructs a Gröbner basis Existence

(b) Reduced Gröbner bases characterize ideals Uniqueness

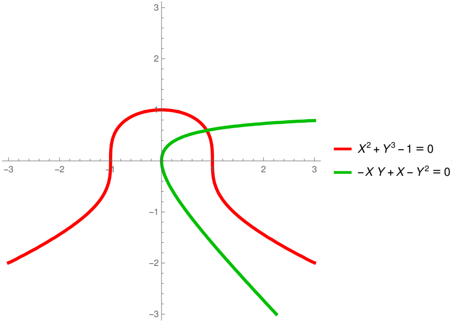
Gröbner theory is widely applicable:

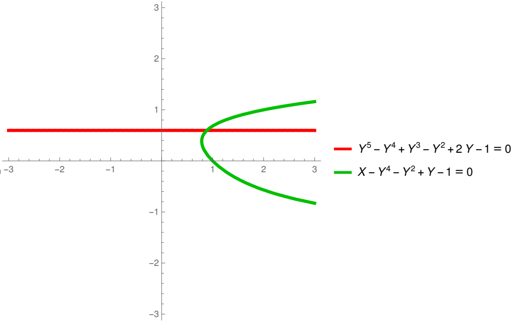
- Applications in computer sciences
- Applications in graph theory
- Applications in theorem proving
- ...

Reduce the complexity!

```
GroebnerBasis[{X^2 + Y^3 - 1, X - Y^2 - X*Y}, {X, Y}]
```

$\{-1 + 2Y - Y^2 + Y^3 - Y^4 + Y^5,\ -1 + X + Y - Y^2 - Y^4\}$





$$\begin{cases} X^2 + Y^3 - 1 = 0 \\ -XY + X - Y^2 = 0 \end{cases} \rightsquigarrow \begin{cases} Y^5 - Y^4 + Y^3 - Y^2 + 2Y - 1 = 0 & \text{Only in } Y \\ X - Y^4 - Y^2 + Y - 1 = 0 & \text{Trivial for fixed } Y \end{cases}$$

Gröbner theory can reduce the complexity by a lot

Thank you for your attention!

I hope that was of some help.