Analogy between $k[x]$ & $\mathbb{Z}$; EDs $\Rightarrow$ dim $= 1$, UFD.

We can extend this to some ring extensions. We compare

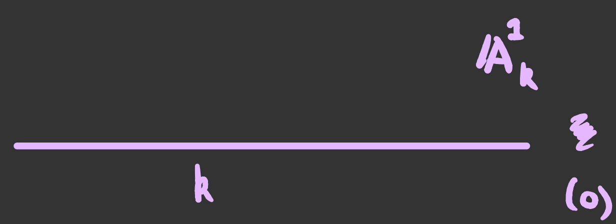
$$B = \mathbb{Z}[\sqrt{-3}] \supseteq \mathbb{Z} = A \quad \& \quad B = \frac{k[x,y]}{y^2 - x^3} \cong k[x][\sqrt{x^3}]$$
$$\cup\!\!\mid$$
$$k[x] = A \,.$$

In both cases, we investigate $\operatorname{Spec} B$ via the map

$$\varphi^*: \operatorname{Spec} B \longrightarrow \operatorname{Spec} A, \quad \text{induced by } \varphi: A \hookrightarrow B.$$
$$\mathfrak{p} \longmapsto \varphi^{-1}(\mathfrak{p}) = \mathfrak{p} \cap A$$

1^{st} // $B = \dfrac{k[x,y]}{y^2 - x^3} \supseteq k[x] = A$ Assume $k = \bar{k}$.

Then $\underset{\mathbb{A}^1_k =}{\operatorname{Spec} k[x]} = \{(x-a) \mid a \in k\} \cup \{(0)\}$



→ & the Nullstellensatz

Then correspondence theorem says that

$$\{ m \trianglelefteq B \} \overset{1:1}{\longleftrightarrow} \{ \tilde{m} \trianglelefteq k[x,y] \mid (y^2 - x^3) \subseteq \tilde{m} \}$$

note since the correspondence respects inclusion, it follows that maximals correspond to maximals. One also shows easily primes correspond to primes.

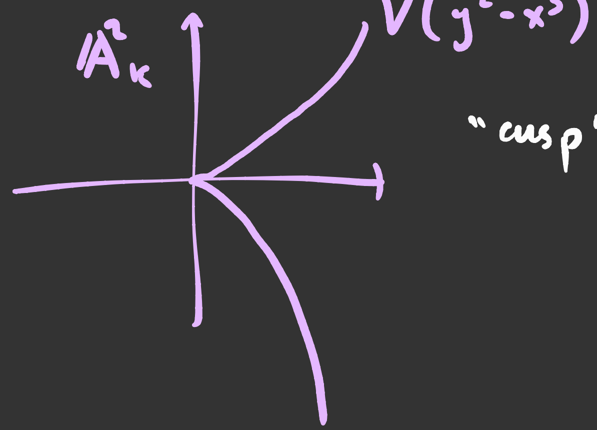
Thus

$$\operatorname{mSpec} B = \{ m_{a,b} = (x-a, y-b) \mid (y^2 - x^3) \subseteq m_{a,b} \}.$$

Then thinking of $m_{a,b} = \ker\left(\begin{array}{ccc} k[x,y] & \xrightarrow{\varphi_{a,b}} & k \\ x & \longmapsto & a \\ y & \longmapsto & b \end{array} \right)$, it

is clear that $(y^2 - x^3) \subseteq m_{a,b} \iff \varphi_{a,b}(y^2 - x^3) = b^2 - a^3 = 0$.

$$\begin{array}{ccccc} \mathbb{A}^2_k & = & \{ (a,b) \in k^2 \} & \overset{1:1}{\longleftrightarrow} & \operatorname{mSpec} k[x,y] \\ \cup\!\shortmid & & \cup\!\shortmid & & \cup\!\shortmid \\ V(y^2 - x^3) & = & \{ (a,b) \mid b^2 = a^3 \} & \overset{1:1}{\longleftrightarrow} & \operatorname{mSpec} B \end{array}$$



Now consider $\varphi : \underset{\overset{\shortparallel}{A}}{k[x]} \hookrightarrow \underset{\overset{\shortparallel}{B}}{\dfrac{k[x,y]}{(y^2-x^3)}}$ &

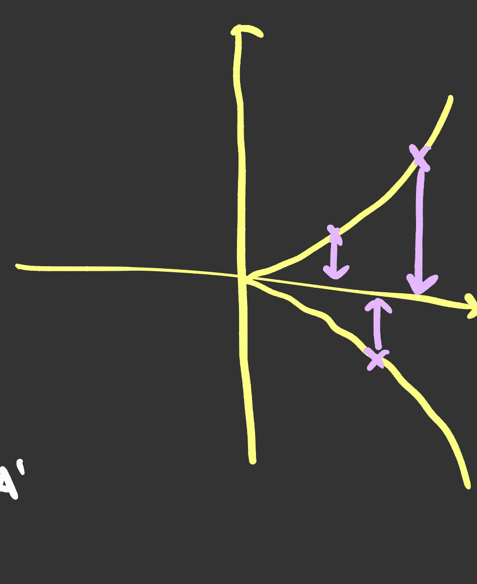
the map $\varphi^* : \operatorname{Spec} B \longrightarrow \operatorname{Spec} A$.

$$\mathfrak{p} \longmapsto \varphi^{-1}(\mathfrak{p}) = \mathfrak{p} \cap A$$

which on maximals: $(x-a, y-b) \cap k[x] = (x-a)$,

Thus

$$\begin{array}{ccc} \varphi^* : \operatorname{mSpec} B & \longrightarrow & \operatorname{mSpec} A \\ \text{\rotatebox{90}{$\cong$}} & & \text{\rotatebox{90}{$\cong$}} \\ V(y^2-x^3) & \longrightarrow & \mathbb{A}^1_k \\ (a,b) & \longmapsto & a \end{array}$$



Is just the projection $pr_1 : \mathbb{A}^2 \to \mathbb{A}^1$

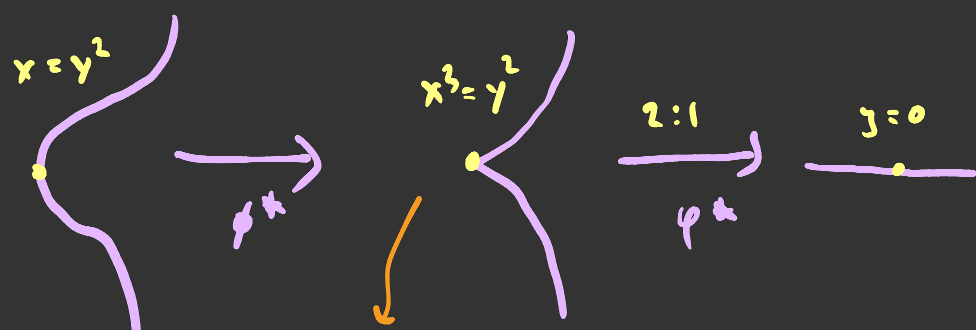
Note, $B = \dfrac{k[x,y]}{y^2 - x^3} \cong k[t^2, t^3] \underset{\phi}{\hookrightarrow} k[t]$,

which we can see as $\underset{\cong \frac{k[x,y]}{(x-y^2)}}{k[x][\sqrt{x}]} \supseteq k[x][\sqrt{x^3}]$ & letting $t = \dfrac{x}{y}$.

Then similar to the calculation above with have

$$\phi^* : \operatorname{mSpec} k[t] \longrightarrow \operatorname{mSpec} B$$
$$a \longmapsto (a^2, a^3).$$

We get



"Resolution" via "normalisation"

Now we do the number theoretic example.

Let $B := \mathbb{Z}[\sqrt{-3}] \supseteq \mathbb{Z} =: A$. Call the inclusion $\iota : \mathbb{Z} \hookrightarrow \mathbb{Z}[\sqrt{-3}]$. Then consider the map

$$\iota^* : \operatorname{Spec} \mathbb{Z}[\sqrt{-3}] \longrightarrow \operatorname{Spec} \mathbb{Z}$$
$$\mathfrak{p} \longmapsto \mathfrak{p} \cap \mathbb{Z}$$

As $\operatorname{Spec} \mathbb{Z} = \{(2), (3), (5), \dots\} \cup \{(0)\}$, we see that $\overset{\neq 0}{\mathfrak{p}} \cap \mathbb{Z} = (p)$ for some prime $p \in \mathbb{Z}$, it's easy to see $(0) \subseteq \mathbb{Z}[\sqrt{-3}]$ is the only ideal s.t. $\iota^*(\mathfrak{p}) = (0)$.

We say $\mathfrak{p}$ lies over p.

From the appendix we know $p = \underset{\mathfrak{p}_+}{(b + a\sqrt{-3})}\underset{\mathfrak{p}_-}{(b - a\sqrt{-3})}$

$\Leftrightarrow \quad p \equiv 1 \mod 6$.

For example, $7 = (2 + \sqrt{-3})(2 - \sqrt{-3})$.

Now I claim $p \neq 2, 3$, then either $p = f_+ \cdot f_-$, $f_\pm$ prime elements, or p prime in B. That is:

$$\left|(\varphi^*)^{-1}(p)\right| \leq 2 .$$

Now let $p \equiv 1 \mod 6 \Rightarrow p = f_+ \cdot f_-$. Consider

$$\begin{tikzcd}
\mathbb{Z}[x] \arrow[r] \arrow[dd] \arrow[rr, bend left, "\alpha"] & \mathbb{Z}[\sqrt{-3}] = B \arrow[r] \arrow[d, phantom, "\cong"] & B/(f_\pm) \\
 & \mathbb{Z}[x]/(x^2+3) \arrow[d] & \\
\mathbb{F}_p[x] \arrow[r] & \mathbb{F}_p[x]/(x^2+3) \arrow[uur, "\beta"] &
\end{tikzcd}$$

induced by the isom. theorem since $\alpha(p) = \alpha(x^2+3) = 0$

Since $p = 3a^2 + b^2 = 0$ in $\mathbb{F}_p$, $\ker(\beta) = \left(x \mp \frac{b^2}{a^2}\right)$

Thus (count elements) $B/f_\pm \cong \mathbb{F}_p$.

Now assume $p \equiv 5 \mod 6$, then p does not factor & $x^2+3 \in \mathbb{F}_p[x]$ is irred, thus

$\frac{\mathbb{F}_p[x]}{x^2+3} \cong \mathbb{F}_{p^2}$. As above we get a map

$$\beta : \frac{\mathbb{F}_p[x]}{x^2+3} \xrightarrow{\cong} \frac{B}{(p)} .$$

$\Rightarrow p$ prime

Lastly, $p = 3 \Rightarrow \frac{B}{(3)} \cong \mathbb{F}_3 \Rightarrow 3$ is prime.

$p = 2$ is bad: $2 \neq (b+a\sqrt{-3})(b-a\sqrt{-3}) \quad \forall a,b \in \mathbb{Z}$

thus is irreducible, but not prime! Indeed,

$$2^2 = (1+\sqrt{-3})(1-\sqrt{-3})$$

(& we know factorisation in primes has to be unique.)

It follows $(\varphi^*)^{-1}((2)) = (2, 1+\sqrt{-3})$ is unique over (2) & needs 2 generators.

As for the cusp we can enlarge this ring:

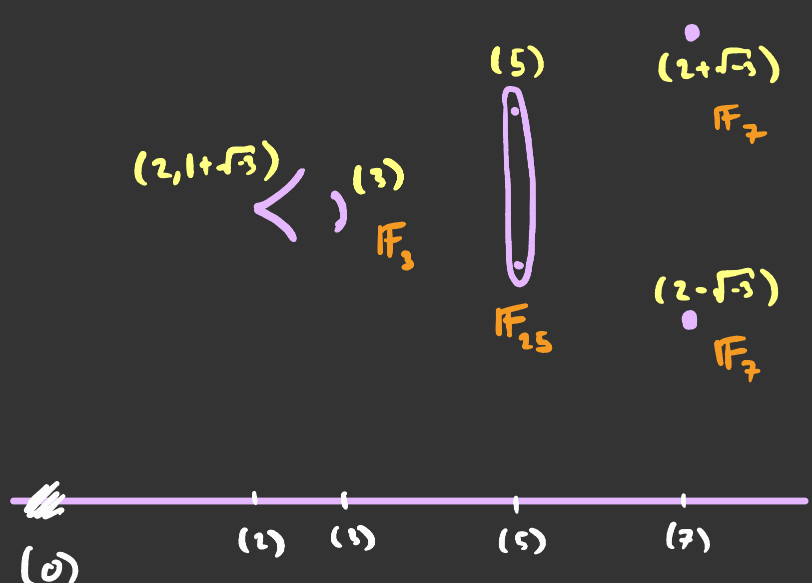
$B' := \mathbb{Z}\Big[\underbrace{\tfrac{1+\sqrt{-3}}{2}}_{=\,\omega}\Big]$, ω primitive root of unity.

Then B' is an ED $\Rightarrow$ UFD.

Now prime analysis is the same as B except over (2) we have $B'/(2) \cong \mathbb{F}_2[x]/(x^2+x+1) \cong \mathbb{F}_4$

As before we can draw a spec picture of $A \subseteq B \subseteq B'$

$$\operatorname{Spec} B' \xrightarrow{\phi^*} \operatorname{Spec} B \xrightarrow{\varphi^*} \operatorname{Spec} A$$



[Reid] says "we draw bubble w/ 2 pts over (5) to have two conjugate pts $X = \pm\sqrt{-3}$ of X-line defined over $\mathbb{F}_{p^2}$".

I don't get this yet.