Warning 1 These are sketchy and incomplete draft lecture notes written for myself for my 256A course.

Course home page http://math.berkeley.edu/~reb/256A
Text: Hartshorne, Algebraic Geometry. We cover same topics, but often different viewpoint. Lectures do not necessarily contain complete proofs.

Example 1 Solve $x^{2}+y^{2}=z^{2}$ in integers. $3^{2}+4^{2}=5^{2}$.
Algebraic solution: Can assume $x, y, z$ coprime, so $z$ is odd, and $x$ (say) is odd.

Then $x^{2}=(z-y)(z+y)$ is a product of coprime factors, so $z-y=r^{2}$, $z+y=s^{2}$, with $r$ and $s$ odd and positive, so $z=\left(r^{2}+s^{2}\right) / 2, y=\left(s^{2}-r^{2}\right) / 2$, $x=r s$. Examples with $(r, s)=(1,3),(1,5),(3,5)$.

Geometric solution: $X=x / z, Y=y / z$, so $X^{2}+Y^{2}=1$. Put $t=y /(x+1)$ DIAGRAM
$t \in \boldsymbol{Q}$ corresponds to solutions other than $(-1,0)$
$Y=t(X+1)$ so $t^{2}(X+1)^{2}+X^{2}=1$, so $(X+1)\left(\left(t^{2}+1\right) X+t^{2}-1\right)=0$ (Must have root at $X=-1$ ), so factors.)
so $X=\frac{1-t^{2}}{1+t^{2}}, Y=\frac{2 t}{1+t^{2}}$
Example: $t=1 / 2, \stackrel{X}{X}=3 / 5, Y=4 / 5$.
This is a BIRATIONAL map from the circle to the line: an isomorphism except in codimension at least $1 .\left(X \neq-1, t^{2} \neq-1\right)$. No analogue for smooth manifolds.

Circle forms GROUP of rotations: product of $\left(x_{1}, y_{1}\right)\left(x_{2}, y_{2}\right)=\left(x_{1} x_{2}-\right.$ $\left.y_{1} y_{2}, x_{1} y_{2}+x_{2} y_{1}\right)$.

Example of ALGEBRAIC GROUP $G$ taking a commutative ring $R$ to a group $G(R)$.

What is $G(\boldsymbol{C})$ ? Answer: For $(x, y) \in G(\boldsymbol{C})$ put $z=x+i y$ (note that $x$ and $y$ are COMPLEX with $x^{2}+y^{2}=1$ ). Then $x-i y=z^{-1}$ so $x=\frac{z+1 / z}{2}$, $y=\frac{z-1 / z}{2 i}$, so $G(\boldsymbol{C})=\boldsymbol{C}^{*}$. Example of a torus splitting over $\boldsymbol{C}$.

Example 2 Solve $y^{2}=x^{3}+x^{2}$
DIAGRAM There is a NODE at $(0,0)$, simplest example of a SINGULARITY.

Put $y=t x .3$ intersection points, 2 at $(0,0)$, so 3 rd must be RATIONAL. $t^{2} x^{2}=x^{3}+x^{2}$, so $x=t^{2}-1, y=t^{3}-t$. Example: $(3,6)$.
$t \rightarrow\left(t^{2}-1, t^{3}-1\right)$ maps $A^{1}$ to curve, $2: 1$ at $0,1: 1$ elsewhere. It is a RESOLUTION of the singularity, and an example of BLOWING UP. (Hironaka resolved all sings in char 0; char ¿0 still open.)

Example 3 Solve $x^{n}+y^{n}=z^{n}$ in rationals. Algebraic geometry over $\boldsymbol{Q}$ is HARD.
Example 4 Solve $x^{3}+y^{3}=9$ in rationals. (Dudeney, Canterbury puzzles $\# 20$; Fermat)

Solution: $\left(\frac{415280564497}{348671682660}\right)^{3}+\left(\frac{676702467503}{348671682660}\right)^{3}=9$. Dudeney found this by hand! How?

No double points, so cannot use previous method. Chord-tangent process leads to new points starting from 2 known points (possibly the same). This almost defines a group $(a+b+c=0 \leftrightarrow a, b, c$ collinear. Identity: add "point at infinity". Example of a PROJECTIVE variety that is a group: ABELIAN variety.

This is NOT birational to $A^{1}$ : it has genus 1 , not 0 as a Riemann surface.
Projective coordinates: $(x: y: z) \bmod \lambda . x^{3}+y^{3}=9 z^{3} . z \neq 1$ : as above. Extra point (1:-1:0).

Associativity hard to prove directly but follows from $a_{1}+\ldots a_{n}=b_{1}+\ldots+$ $b_{n} \leftrightarrow$ there is a rational function with zeros at a's, poles at $b$ 's.

Tangent to $(a, b)$ is $y=-\frac{a^{2}}{b^{2}}(x-a)+b$. So $x^{3}+\left(-\frac{a^{2}}{b^{2}}(x-a)+b\right)^{3}=9$. Cubic in $x$ with 2 roots $a$, and product of roots $=-$ constant term/leading term , so third root is $-\left(\left(9 / b^{2}\right)^{3}-9\right) / a^{2}\left(1-a^{6} / b^{6}\right)=\left(9 b^{6}-9^{3}\right) / a^{2}\left(b^{6}-a^{6}\right)$. For $(a, b)=(1,2)$ this gives $(-17 / 7,20 / 7)$.

Cubic curves are examples of abelian varieties: connected projective algebraic groups. Abelian varieties are abelian (proof for complex numbers: any map from projective variety to $\boldsymbol{C}$ is constant by maximum principle, so adjoint map to automorphism group of tangent space of origin is 0 .) Warning: abelian linear groups are NOT abelian: this is a old name for the sympectic group, an affine algebraic group.

Singular cubics such as $y^{2}=x^{2}+x^{3}$ also have a group law on singular points, though this is affine not projective.

Example 5 Bezout's theorem. Essentially first proved by Newton??? (check this)

Example 6 Pappus's theorem. One of the 2 interesting theorems about lines. DIAGRAM of Pappus's theorem
Special case of:

Example 7 Pascal's theorem.

## DIAGRAM

$\ell_{1} \cap \ell_{4}, \ell_{2} \cap \ell_{5}, \ell_{3} \cap \ell_{6}$ collinear (Pascal line)
Proof via algebraic geom: Pick $P$ on conic. Choose $\lambda$ with $p_{1} p_{3} p_{5}-\lambda p_{2} p_{4} p_{6}=$ 0 on $P$. $\left(p_{i}=0\right.$ is $\left.\ell_{i}\right)$

Then this is a cubic intersecting the conic in $7>2 \times 3$ points, so must have a component in common by Bezout, which must be the conic. So cubic factors as the conic times a line, which is the Pascal line.

Example 827 lines on a cubic surface.
Example: Fermat surface $w^{3}+x^{3}+y^{3}+z^{3}=0$ in $P^{3}$. Typical line: $(1:-1:$ $t:-t)$. Acted on by group of permutation, multiplying coordinates by cube root of 1 , order $3^{3} 4$ !. 27 images under this group.

Example 9 Dini's proof of finite field Kakeya conjecture: size of Kakeya set in $F^{n}$ is at least $c_{n}|F|^{n}$. Kakaya set: any set containing a line in every direction (unit line for Euclidean space, full line for finite fields).

Besicovich showed that a needle can be turned inside a set of arbitrarily small area; these sorts of questions are important in higher dimensional harmonic analysis, and the finite field case was an analogue suggested by Wolfe.
Proof first show that a Kakeya set cannot lie in hypersurface of degree less than $|F|$. If $f$ is the polynomial of degree $d<|F|$ defining the algebraic set and $f_{d}$ its highest degree component, then for all $v$ we can find $x$ such that $f(x+v t)$ vanishes for all $t \in F$, so the coefficient $f_{d}(v)$ of $t^{d}$ vanishes. As this is true for any $v$ and $f_{d}$ has degree less than $|F|$, we have $f_{d}=0$, so $f=0$. (A polynomial of degree less than $|F|$ cannot vanish at all points of $F$, though a polynomial of degree $|F|$ such as $x^{|F|}-x$ can.)

Next observe that polynomials of degree $\leqslant d$ in $n$ variables have dimension $\binom{n+d}{n}$ so we can find a hypersurface of degree at most $d$ containing any set with less than this many elements. So any Kakaya set has at least $\binom{n+|F|-1}{n} \geqslant|F|^{n} / n$ ! elements.

Affine scheme: something like zeros of polynomials. Scheme: covered by affine schemes (example: $P^{3}$ ). Compare with definition of differentiable manifold.

Vector bundles in differential geometry: functions, differential forms, tangent fields, etc. For schemes use SHEAVES (cotangent bundle of something with a singularity does not exist, but its cotangent sheaf does.

## 1 Varieties

### 1.1 Affine varieties

$k=$ field. Affine space $=k^{n}=A^{n}$.
Algebraic set $Y=$ zeros of a set $T$ of polynomials: $Y=Z(T)$
Closed under finite union, arbitrary intersection. So form closed sets of ZARISKI TOPOLOGY on $k^{n}$.

Example $10 A^{1}$ Closed sets=finite subsets, whole space. NOT HAUSDORFF!
Example $11 A^{2}$ Closed sets: points, curves, whole space. (DIAGRAM) Zariski topology is NOT product topology (DIAGRAM)

Example 12 Determinantal varieties. $A^{m n}=m \times n$ matrices $=$ linear maps from $k^{n} \rightarrow k^{n}$. Subset of matrices of rank $\leqslant N$ is an affine subvariety, given by matrices such that all minors of rank $N+1$ vanish. In particular the subset of maps $k^{m} \rightarrow k^{n}$ that are onto is open.

Recall $k\left[x_{1}, \ldots, x_{n}\right]$ is Noetherian. Recall 3 conditions for Noetherian ring: every ideal f.g., every ascending chain stabilizes, every set of ideals has a maximal element.
Proof $R$ Noetherian implies $R[x]$ Noetherian. Look at ideal $I_{0} \subseteq I_{1} \subseteq \ldots \subseteq$ $I_{n} \subseteq \ldots$ of leading coefficients of polynomials in $I$ of degree at most $n$. Stabilizes at $N$ say, so $I$ generated by its polynomials of degree at most $N$.

Exercise 1 Show that if $R$ is Noetherian then so is $R[[x]]$.
Topological space called Noetherian if closed sets satisfy descending chain condition.

So $A^{n}$ is Noetherian because $k\left[x_{1}, \ldots, x_{n}\right]$ is Noetherian.
Noetherian equivalent to every open set is compact. (or quasicompact in Bourbaki's terminology). Noetherian+Hausdorff implies finite: (complement of a point is open, so compact, so closed, so points are open).

A set is called IRREDUCIBLE if it is nonempty and not the union of proper closed subsets. In a Noetherian space, every closed set is a finite union of irreducible closed subsets (proof by Noetherian induction: look at minimal closed counterexample). This is a refinement of decomposition into connected components: for example $x y=0$ is connected but reducible.

Example $13 x^{2}+y^{2}+z^{2}=0, x y z=0$. Union of 6 lines $x=0, y= \pm i z$, etc.
Example $14 x y=1$ has only 1 irreducible component over $\boldsymbol{R}$. Irreducible components are connected in Zariski topology, but need not be connected in usual topology! (It is connected over $\boldsymbol{C}$.)

Example 15 Families of mostly irreducible algebraic sets can have reducible members. For example, look at intersection of $\mathrm{xy}=z$ with $z=c$ : this is irreducible for $c \neq 0$, but a union of 2 lines for $c=0$. (DIAGRAM)

Definition 1 (provisional) An affine variety is an irreducible closed subset of affine space.

This definition is in fact a bit misleading: it turns out that the non-zero points of the affine line also form an affine variety, as they are isomorphic to an affine variety $x y=1$, so we will later modify it.

Nullstellensatz: What is relation between
(1) Subsets $Y$ of $A^{n}$
(2) Ideals $I$ of $k\left[x_{1}, \ldots, x_{n}\right]$ ?
$Y \rightarrow I(Y)=$ polynomials vanishing on $Y$
$Z(a) \leftarrow a$ zeros of polynomials in ideal $a$.
$Z(I(Y))$ is closure of $Y$ by definition.
Is $I(Z(a))=a$ ? NO! $a=\left(x^{2}\right), I(Z(a))=(x)$. More generally, if $f^{n} \in a$ then $f \in I(Z(a))$ so $\sqrt{a} \subseteq I(Z(a))$.

Is $I(Z(a))=\sqrt{a}$ ? No! Over $\boldsymbol{R}$, take $a=\left(x^{2}+y^{2}+1\right)$ so $Z(a)=\varnothing$.

First look at easier case of maximal ideals.
What ideals do points correspond to? $\left(a_{1}, \ldots\right) \rightarrow\left(x_{1}-a_{1}, \ldots, x_{n}-a_{n}\right)$ (max ideal).Do all maximal ideals come from points? NO! $\left(x^{2}+1\right)$ is maximal in $\boldsymbol{R}[x]$.

Problems in last 2 examples caused because $\boldsymbol{R}$ is not algebraically closed.
Theorem 1 (Weak Hilbert nullstellensatz: zeros position theorem). If $k$ is algebraic closed, then any max ideal I of $k\left[x_{1}, \ldots, x_{n}\right]$ is of the form $\left(x_{1}-\right.$ $\left.a_{1}, \ldots, x_{n}-a_{n}\right)$.

Proof We know that $K=k\left[x_{1}, \ldots, x_{n}\right] / I$ is a field. Renumber so that $x_{1}, \ldots x_{i}$ are algebraic independent, and remaining ones are algebraic over them. We have
$k \subseteq F=k\left(x_{1}, \ldots x_{i}\right) \subseteq K$
where $K$ is a finite module over $F$ and $F$ is a finitely generated field extension over $k$. We want to show that $F$ is finitely generated as a $k$ algebra (it is trivially finitely generated as a $k$ field!) Note difference between being finitely generated as a field or ring or module: these are all quite different!

Pick $y_{1}, \ldots, y_{m}$ as basis for the $F$-module $K$. Then
$x_{a}=\sum t_{a, b} y_{b}$
$y_{a} y_{b}=\sum t_{a, b, c} y_{c}$
for some t's. Let $T$ be $k$-algebra generated by the $t$ 's, so
$k \subseteq T \subseteq F \subseteq K$
The first extension is a finitely generated algebra extension, the second a finitely generated field extension, and the third a finitely generated module.

Then $T$ is Noetherian as the number of $t$ 's is finite. Moreover $K$ is generated by the $y$ 's as a $T$-module, as this module contains the $x$ 's and is closed under multiplication. So $K$ is a finitely generated module over the Noetherian ring $T$, so its submodule $F$ is also a finitely generated module over $T$, so $F$ is a finitely generated $k$-algebra (this is much stronger than saying it is a finitely generated field extension).

But if $F$ is finitely generated by the elements $f_{j} / g_{j}$ and $i>0$ choose some irreducible polynomial $P$ in $k\left[x_{1}, \ldots x_{i}\right]$ not dividing any $g_{i}$, using the fact that there are infinitely many primes (Euclid). Then $1 / P$ is not in $k\left[f_{1} / g_{1}, \ldots\right]$. This is a contradiction so $i=0$ so $k=F$. Therefore $K$ is a finite extension of the field $k$.

So far we have not used the fact that $k$ is algebraically closed. Finally we use fact the $k$ is algebraically closed to deduce that $K=k$. So each $x_{j}=a_{j}$ for some $a_{j} \in k$.

Theorem 2 Strong Nullstellensatz. If $k$ is algebraic closed then $\sqrt{a}=I(Z(a))$.

## Proof

It is trivial that $\sqrt{a} \subset I(Z(a))$. Rabinowitsch trick: add extra variable $x_{0}$ to deduce strong from weak nullstellensatz. Suppose $a$ is generated by
$f_{1}, \ldots, f_{m}$. Suppose $f \in I\left(Z(a)\right.$ so that $f$ vanishes whenever $f_{1}, \ldots, f_{m}$ vanish. Then $f_{1}, \ldots, f_{m}, 1-x_{0} f$ have no zeros in $A^{n+1}$, so are not in any max ideal by weak nullstellensatz, so its ideal contains 1 . So

$$
1=g_{0}\left(1-x_{0} f\right)+g_{1} f_{1}+\ldots+g_{m} f_{m}
$$

for some $g$ 's. Now put $x_{0}=1 / f$. We get $1=g_{1} f_{1}+\ldots+g_{m} f_{m}$ in the field of rational functions. Clear denominators of the $g$ 's by multiplying by some power of $f$ to get

$$
f^{N}=h_{1} f_{1}+\ldots+h_{m} f_{m}
$$

where $N$ is the max power of $x_{0}$ in the $g$ 's. But this just says that $f \in \sqrt{a}$.
So we get a $1: 1$ correspondence
Closed sets of $A^{n} \leftrightarrow$ Radical ideals $a$ of $k\left[x_{1}, \ldots, x_{n}\right] a=\sqrt{a}$.
Example 16 Intersection of line $y=0$ with parabola $y=x^{2}$ (DIAGRAM). Ideal generated by 2 ideals is $\left(y, y-x^{2}\right)=\left(y, x^{2}\right)$ NOT radical! $\sqrt{\left(y, x^{2}\right)}=$ $(y, x)$. Ideal generated by 2 radical ideals need not be radical.

Example 17 Look at ideal generated by a condition that an $n \times n$ matrix is nilpotent (given by $n^{2}$ polynomials of degree $n$ in $n^{2}$ matrices). This ideal is NOT radical: for example by the Nullstellensatz its radical contains the trace, as if a matrix is nilpotent it has trace 0 . For 2 by 2 matrices the smallest power of the trace in the ideal is the cube (not the square as one might guess). It can be really hard to find the radical of an ideal, or even tell if an ideal is radical; this seems to be an open problem for the ideal saying that 2 matrices commute. (The "moduli space" of pairs of commuting matrices is a notoriously hard space to understand!)

Refinement for schemes: Lasker-Noether theorem says that any ideal of a Noetherian ring is intersection of primary ideals. Lasker's definition of primary was that $a b \in \mathfrak{p} \rightarrow a \in \mathfrak{p} \vee b \in \sqrt{\mathfrak{p}}$. It turns out to be more convenient to focus on the MODULE $R / I$ rather than the IDEAL $I$. Recall that an associated prime of a module is a prime ideal that is the annihilator of some nonzero element. (Any maximal element of set of annihilators of elements is prime, as if $I$ is the annihilator of $m$ and $\mathrm{xy} \in I$ then either $y m=0$ so $y \in I$ or $x$ is in the annihilator of $\mathrm{ym} \neq 0$ so $x \in I$ as I is maximal. In general maximal elements of sets of ideals have a strong tendency to be prime.) For N rings one can show that an ideal is primary in Lasker's sense if and only if the module $R / I$ has exactly one associated prime, and it is convenient to adopt this property as a definition: a module is called COPRIMARY if it has exactly 1 associated prime. (A submodule is called primary if the quotient is coprimary, but this depends on 2 modules rather than 1.) Better viewed as a theorem about finitely generated modules over Noetherian rings: 0 is intersection of primary submodules. (proved by world chess champion Lasker for ideals in polynomial and power series rings, generalized by Noether and Grothendieck to coherent sheaves over Noetherian schemes.) Special case: finite abelian groups. Lasker's
original paper proving the special case of ideals in polynomial rings was about 100 pages long, involving a complicated induction on dimension. The more general theorem about modules over Noetherian rings can be proved in a few lines as follows. (This shows the advantage of using the "correct" definitions: they almost force you to write down the simple proof.)

Proof: 1. in any Noetherian module, 0 is intersection of finite number of irreducible submodules (irreducible $=$ not intersection of 2 larger submodules), as by Noetherian induction if it is not there is a max submodule that is not, which gives a contradiction. 2. Any irreducible submodule is a primary submodule. Equivalently if 0 is irreducible in $M$ then $M$ is coprimary. This follows because if $\mathfrak{p}, \mathfrak{q}$ are associated primes then there are submodules $R / p, R / \mathfrak{q}$ which have zero intersection, as annihilator of any nonzero element of these submodules is $\mathfrak{p} \neq \mathfrak{q}$.

Exercise 2 Check that, for Noetherian rings, if $R / \mathfrak{q}$ is coprimary then $\mathfrak{q}$ is primary in Lasker's sense.

Hints: (1) First reduce to the case $\mathfrak{q}=0$.So we have to show that if $\mathfrak{p}$ is the only associated prime of $R$ then it is nilpotent, or equivalently every element is nilpotent. (2) If $a \in \mathfrak{p}$ is not nilpotent then $R_{a} \neq 0$, so pick an associated prime of $R_{a}$. Show that its inverse image in $R$ is prime, and is the annihilator of $a^{n} b$ for some $n$. Deduce that is an associated prime of $R$ but does not contain $a$, and obtain a contradiction.

Example 18 Look at the ideal generated by ( $\mathrm{xy}, y^{2}$ ). The algebraic set is just $y=0$ but this does not give a complete picture of the ideal: informally there is a little bit sticking out at the origin. A primary decomposition of this ideal is the intersection of the ideals $(y)$ and $\left(x, y^{2}\right)$. This primary decomposition is not unique, even if we remove redundant elements and have only one primary ideal for each prime: it can also be given as the intersection of $(y)$ and $\left(x+y, y^{2}\right)$. So a minimal decomposition into irreducible algebraic sets is unique, but we do NOT get uniqueness for the more general case of ideals or subschemes. The "point with a bit sticking out" is called an embedded component, meaning that its underlying algebraic set is contained in the algebraic set of a larger irreducible component. In general the primary ideals of the "maximal"irreducible algebraic sets are unique, while the primary ideals of the embedded components need not be (though their radicals are uniquely determined).

Example 19 Primary decomposition is a generalization of the structure theorem for finitely generated abelian groups: if $M$ is the sum of $Z^{n_{0}}$ and $p$-groups for various $p$ then 0 is the intersection of the primary submodules whose quotients are $Z^{n_{0}}$ and the $p$ groups. Note that this decomposition is unique for FINITE groups but not unique in general: for example $Z+Z / 2 Z$ has more than 1 such decomposition. As a special case we "generalize" the fundamental theorem of arithmetic: primary decomposition of $Z / n Z$ closely related to the factorization of $n$ into primes.

Warning: primary is not the same as power of a prime. For example, in $k[x, y]$ any ideal containing some power of $(x, y)$ is primary, but need not be a
power of $(x, y)$.
So affine varieties correspond to finitely generated algebras over $k$ with no nilpotents. Application: can we take quotient $V / G$ of affine variety $V$ by a group $G$ ? Taking quotient of points is unclear: how do we make this an affine variety? Idea: coordinate ring of $V / G$ should be invariant elements of coordinate ring of $V$. This is obviously an algebra over $k$ with no nilpotents. Is it finitely generated? A: Sometimes (Hilbert) but not always (Nagata).

Example 20 Consider affine space $A^{n}$ acted on in the obvious way by the symmetric group $S_{n}$ permuting coordinates. The quotient has coordinate ring the symmetric polynomials, which is a polynomial ring in the elementary symmetric polynomials. So the quotient is affine space again. (It is unusual for a quotient to be so well behaved: this happens for (complex) reflection groups.) The quotient my not be what you expect: for example if we take the quotient of the real affine line by $z \rightarrow-z$ the quotient has coordinate ring $R\left[x^{2}\right]$ so the quotient is again the affine line, which seems wrong as this is not the topological space quotient. The reason is that the quotient is really pairs of points $\{z,-z\}$ fixed by complex conjugation, which includes things like $\{i,-i\}$.

Example 21 Orthogonal group has ring of invariants generated by $(x, x)$, a polynomial ring in 1 variable, corresponding to the fact that the quotient (set of spheres centered at the origin) is the affine line. The special linear group of $V$ acting on $V^{n}$ has no nontrivial invariants for $n<\operatorname{dim}(V)$ as in this case the group acts transitively on a dense open set ( $n$ linearly independent vectors). But for $n=\operatorname{dim}(V)$ the determinant is an invariant.

Example 22 Classical invariant theory: $G=\mathrm{SL}_{2}(\boldsymbol{C})$ acting on $a_{n} x^{n}+a_{n-1} x^{n-1} y+$ $\ldots+a_{0} y^{n}, A=\boldsymbol{C}\left[a_{0}, \ldots, a_{n}\right] . A^{G}$ is the ring of invariants of binary forms, shown to be finitely generated by Gordan. More complicated examples in more variables shown to be finitely generated by Hilbert. Example of an invariant: the discriminant $b^{2}-4 a c$ of $\mathrm{ax}^{2}+\mathrm{bxy}+\mathrm{cy}^{2}$.
(Gordan is supposed to have said about Hilbert's finiteness proof "this is not math; this is theology" as Hilbert's proof was not constructive. It is not al all clear if he really said this, and in any case it may have been a compliment rather than a complaint; Gordan thought highly of Hilbert's work.)
Proof We do the case when $G$ is finite. $A$ is graded by degree. Let $I$ be ideal generated by positive degree elements of $A^{G}$. Then $I$ is a finitely generated ideal by Hilbert basis theorem, with generators $i_{1}, \ldots, i_{k}$ which we can assume are fixed by $G$. We want to show that these generate $A^{G}$ as an ALGEBRA, which is much stronger than saying they generate IDEAL $I$. (Example: subring of $k[x, y]$ generated by $x y^{*}$ is NOT finitely generated, even though corresponding ideal is. We need to use some special property of subrings fixed by a finite group.)

Need Reynolds operator $\rho$ given by taking average under action of $G$ (needs char $=0$ ). Key properties: $\rho(\mathrm{ab})=a \rho(b)$ if $a$ fixed by $G, \rho(1)=1$. Not true that
$\rho(\mathrm{ab})=\rho(a) \rho(b)$ in general. $\rho$ is a projection of $A^{G}$ modules from $A$ to $A^{G}$ but is not a ring homomorphism.

We show by induction on degree of $x$ that if $x \in A^{G}$ then it is in algebra generated by $i$ 's.

We know

$$
x=a_{1} i_{1}+\ldots+a_{k} i_{k}
$$

for some $a$ 's in $A$ as $x$ is in $I$. Apply Reynolds operator:

$$
x=\rho(x)=\rho\left(a_{1}\right) i_{1}+\ldots+\rho\left(a_{k}\right) i_{k}
$$

By induction $\rho\left(a_{j}\right)$ is in $A^{G}$ as it has degree less than that of $x$, so $x \in A^{G}$.
Compact groups: similar as can still integrate over the group:
Noncompact groups such as $\mathrm{SL}_{n}(\boldsymbol{C})$ : Use Weyl's unitarian trick: invariant vectors (for finite dimensional complex reps of the complex group) same as for compact subgroup $\mathrm{SU}_{n}$, so still get Reynolds operator. Works for all semisimple or reductive algebraic groups (key point: reps are completely reducible), but NOT for some unipotent groups (Nagata counterexample to Hilbert conjecture: take $k$ acting unipotently on $k^{2}$, and copy this 16 times to get $k^{16}$ acting on $k^{32}$. Then the ring of invariants of a "generic" 13-dimensional subspace of $k^{16}$ is not finitely generated.). Char p harder as groups need not be completely reducible; e.g. $Z / \mathrm{pZ}$ acting on 2 -dim space over $\boldsymbol{F}_{p}$. Haboush proved Mumford's conjecture giving a sort of nonlinear analogue of Reynolds operator, which can be used to prove finitely generated of invariants for reductive groups as in char 0 . Summary: quotient of affine variety by reductive group is affine variety.

Quotients by groups are used in constructing moduli spaces: for example (moduli space of elliptic curves) is roughly (Hilbert scheme of cubic curves in $\left.P^{2}\right) /\left(\right.$ action of group of automorphisms of $\left.P^{2}\right)$

Example 23 Hyperelliptic curves $y^{2}=a_{n} x^{n}+\ldots+a_{0}$. Rewrite this as $y^{2} z^{n-2}=a_{n} x^{n} z_{0}+\ldots+a_{0} x^{0} z^{n}$. The group $\mathrm{SL}_{2}(k)$ acts on the space of degree $n$ forms in $x$ and $z$. We want to find the quotient space, which will be closely related to the moduli space of hyperelliptic curves. The coordinate ring is the space of all invariant polynomials in $a_{0}, \ldots, a_{n}$; in other words we want to know the invariants of binary quantics. (These are finitely generated by Gordan's theorem.)

Example 24 Cyclic quotient singularities. Take quotient of a cyclic group acting on a vector space. Example: cyclic group of order $n$ acting on $A^{2}$ by $(x, y) \rightarrow(\zeta x, \zeta y)$ where $\zeta$ is a primitive $n$th root of 1 . The invariant polynomials are generated by the $n+1$ elements $z_{i}=x^{i} y^{n-i}$. There are many relations between them as $z_{i} z_{j}=z_{k} z_{l}$ whenever $i+j=k+l$.

Example 25 (Suggested by Petya on mathoverflow from Kontsevich) A moduli space as a quotient. Look at configuration of cyclohexane: chemist Hermann Sachse in 1890 discovered that there are 2 forms of this. Take a cycle of 6
unit lines in $\boldsymbol{R}^{3}$ such that each meets the next at some fixed angle, say right angles. (Cyclohexane has angle about 109 degrees.) The configuration space is affine variety given by intersection of 12 quadrics in 18 dimensional space. Moduli space of configurations is quotient of this by 6 -dimensional group of Euclidean motions, so we might incorrectly guess it has dimension 0 . There are two components, one ("chair") of dimension 0 invariant under inversion through origin (omit opposite vertices of a cube) and one of dimension 1 invariant under rotation by half a revolution (omit adjacent vertices of a cube.) This is flexible because one can fix 3 consecutive edges then rotate this by $1 / 2$ revolution to make endpoints meet. There are similar statements for almost any edges $a, b, c, a, b, c$ and angles $\alpha, \beta, \gamma, \alpha, \beta, \gamma$, though there can sometimes be extra configurations invariant under a reflection exchanging 2 opposite vertices.

Dimension. Intuitively obvious but hard to define and work with.
Hausdorff spaces have following examples:
Cantor showed that there is a bijective map from $\boldsymbol{R} \rightarrow \boldsymbol{R}^{2}$.
Peano curve is a continuous surjective map from $\boldsymbol{R} \rightarrow \boldsymbol{R}^{2}$.
Lebesgue covering dimension: any open cover has a refinement with no point in more than $n+1$ sets means dimension is at most $n$. Example: dimension 2 (DIAGRAM) no point in more than 3 sets. Not trivial to prove that $n$-dim space has dimension $n$.

Dimension for non-Hausdorff spaces is TOTALLY different. Dimension defined as $\sup n$ such that $Z_{0} \subset Z_{1} \subset \ldots \subset Z_{n}$ are distinct and irreducible. DIAGRAM pt $\subset$ curve $\subset A^{2}$

Warning: Any Hausdorff space has dim 0 with this definition, as only irreducible sets are points. On the other hand, $A^{1}$ has infinite Lebesgue covering dimension, as any finite number of non-empty open sets intersect. So NO relation between two definitions of dimension.

Problem: What are irreducible subsets of (say) $A^{4}$ ? Hard to describe, and one needs nontrivial commutative algebra to calculate dimension.

Dimension of a ring: Dimension defined as sup $n$ such that $P_{0} \subset P_{1} \subset \ldots \subset$ $P_{n}$ are distinct prime ideals. $\operatorname{Dim} R=\sup \operatorname{dim} R_{m}, m$ maximal, so can be reduced to dimension of local rings.

Algebraic definition: main idea is that higher dimensional spaces have more functions on them.

Example $26 \operatorname{dim} B / k=\operatorname{tr}$. deg. ring of quotient field of $B$ over $k$.
Example 27 Best definition uses Hilbert polynomial of a local ring. Look at $\operatorname{dim}\left(A / m^{k}\right)$ : this is a polynomial in $k$ for large $k$ of degree $d$, and $d$ is the dimension of the local ring. It is also the same as the dimension of the completion as these have the same Hilbert polynomials.

For example, $k\left[x_{1}, \ldots, x_{n}\right]$ has dimension $n . ~ k[x, y] /\left(y^{2}-x^{3}-a x-b\right)$ has dimension 1.

Warning 2 Noetherian local rings always have finite dimension, but Noetherian rings can have infinite dimension. Non-Noetherian rings can have dimension 0 (example: $\left.k\left[x_{1}, \ldots, x_{n}, \ldots\right]\left(x_{i}^{2}\right)\right)$ so Noetherian is not the same as finite dimensional.

Example 28 Dimension of Hilbert scheme of $n$ points in $A^{m}$ (ideals in $k\left[x_{1}, \ldots, x_{m}\right]$ with codimension $n$ ). Obvious guess for dimension is $m n$ as Hilbert scheme seems to be a sort of symmetric product of $A^{m}$. This is correct for $m=1,2$ but fails horribly for larger $m$. Example: take $m=3$ and look at ideals $I$ with $\mathfrak{m}^{k} \supseteq I \supseteq \mathfrak{m}^{k+1}$ with $\mathfrak{m}=\left(x_{1}, x_{2}, x_{3}\right)$. Any subspace of the vector space $\mathfrak{m}^{k} / \mathfrak{m}^{k+1}$ will give such an ideal. The ideal $\mathfrak{m}^{k}$ has codimension a degree 3 polynomial in $k$ so $\mathfrak{m}^{k} / \mathfrak{m}^{k+1}$ has dimension given by a degree 2 polynomial. So the Grassmannian of subspaces of about half this dimension has dimension given by a degree 4 polynomial $Q$ in $k$, and corresponds to ideals whose codimension is a degree 3 polynomial $P$ in $k$. As $Q(k)$ is eventually larger than $3 P(k)$ there are components of dimension $Q(k)$ greater than $3 P(k)=m n$ when $n$ (number of points) is large enough. In particular there are 0 -dimensional subschemes of degree $n$ that cannot be obtained as limits of $n$ points.

### 1.2 Projective varieties

Definition 2 Projective space $P^{n}=1$-dim subspaces of $k^{n+1}=$ nonzero points ( $x_{0}: \ldots: x_{n}$ ) modulo scalar.

Projective space contains affine space ( $1: x_{1}, \ldots, x_{n}$ ) together with the points at infinity forming a copy of projective space of lower dimension. It is a sort of compactification of affine space (at least over $\boldsymbol{C}$ ). It is covered by $n+1$ copies of affine space.

Historical background. Projective geometry was the study of properties invariant under projection. For example, projection of a railway track onto a picture of a railway track shows that "parallel" lines might meet after projection. (DIAGRAM).

Analytic geometry (using coordinates) versus synthetic geometry (uses axioms about points lines, incidence relations,etc.)

Axioms for synthetic projective geometry: points+lines+incidence relation.

1. Any 2 distinct points meet a unique line.
2. Any 2 lines "in same plane" meet in a point. "In same plane" means they meet 2 intersecting lines in 4 points. (DIAGRAM)
3. Non-degeneracy: any line meets at least 3 points. (Just to eliminate reducible unions.)

- Dim 0: 1 point, no lines., boring.
- Dim 1: just 1 lines, with all points on it. Also boring.
- Dim 2: Any 2 lines meet in a point, at least 2 lines. Projective plane. Example: Fano plane (DIAGRAM).
- $\operatorname{Dim} \geqslant 3$ There exist 2 lines that do not meet.

Examples: points, lines $=1,2$ dimensional subspaces of a vector space over a division ring.

Theorem 3 Desargues. 2 triangles abc, $A B C$ with $a A, b B, c C$ meeting at $E$. Suppose $x$ lies on $b c, B C ; y$ lies on $a c, A C$, and $z$ lines on $a b, A B$. Then $x, y, z$ are collinear

Proof In $\boldsymbol{R}^{3}$. xyz all lie in plane abc and in plane ABC , so they lie in the intersection which is a line if the 2 triangles are not coplanar. General case: project from non-coplanar triangles. This proof FAILS in 2-dimensions!

Remark 1 Another theorem whose proof uses the same trick of looking in 3 dimensions says that if we draw pairs of lines from three circles their intersection points lie on a line.

## Theorem 4

- Any projective space of dimension at least 3 satisfies Desargues theorem.
- Any projective space of dimension at least 2 satisfying Desargues theorem is a projective space over a division ring.
- And the division ring is a field if and only if Pappus's theorem holds.

So projective space are points and lines (boring), non-desarguesian planes and projective spaces over division rings. Non-Desarguesian planes seem to be mostly junk. Examples are the projective plane over the octonions, the projectivization of the Moulton plane (double slopes of lines as the cross the y-axis), finite planes of order $9, \ldots$. Hard problem: is there a projective plane of order n for $\mathrm{n}=10$ (no), 12 (open)...

Summary: synthetic projective geometry + Pappus leads to the definition of projective space used here.

Remark: it is common in math for the case of dim at least 3 to be the general case, the case of dimension 1 is trivial in some sense, and dim 2 is a mess. Examples: Tits buildings classified in terms of algebraic groups for rank at least 3. The notorious quasi-thin case in classification of finite simple groups was a "rank 2" problem.

Affine space $A^{n} \Leftrightarrow k\left[x_{1}, \ldots, x_{n}\right]$
Affine algebraic set $\Leftrightarrow$ radical ideal
Projective space $P^{n} \Leftrightarrow$ GRADED ring $k\left[x_{0}, x_{1}, \ldots, x_{n}\right]$
Affine algebraic set $\Leftrightarrow$ GRADED radical ideal other than $\left(x_{0}, \ldots x_{n}\right)$.
Cone on projective variety=affine variety in $A^{n+1}$.

Example 29 Twisted cubic $T=\operatorname{points}\left(t, t^{2}, t^{3}\right)$ in $A^{3}$, given by ideal ( $y-$ $\left.x^{2}, z-x^{3}\right)$. In $P^{3}$ it is given by the points $\left(s^{3}: s^{2} t: \mathrm{st}^{2}: t^{3}\right)$. Homogenizing the generators gives the graded ideal ( $\mathrm{wy}-x^{2}, w^{2} z-x^{3}$ ) which is NOT the full ideal ( $\mathrm{wy}-x^{2}, y^{2}-\mathrm{xz}, \mathrm{wz}-\mathrm{xy}$ ) of the projective curve. In particular $\mathrm{wz}-\mathrm{xy}$ is not in the ideal generated by wy $-x^{2}, w^{2} z-x^{3}$. In fact the latter ideal is not even reduced. Analyze it on the 4 affine spaces covering projective space:

- $w=1$ : we get the affine twisted cubic of degree 3 .
- $x=1$ : we get wy $=1, w^{2} z=1$ so again we just get a single curve (affine line - point).
- $y=1$ : we get $w=x^{2}, w^{2} z=x^{3}$. Eliminating $w$ gives $x^{4} z=x^{3}$ which splits as $\mathrm{xz}=1$ and $x^{3}=0$. So we get a sort of triple copy of the line $w=x=0$ as well as the twisted cubic.
- $z=1$ : We get wy $=x^{2}, w^{2}=x^{3}$. Eliminating $y$ gives $w^{2}=x^{3}$. However we can only eliminate $y$ like this when $w$ is nonzero, and we pick up an extra line. Eliminating $y$ gives $x^{4}=x^{3}$ so this line has multiplicity 3 again.

The decomposition of the variety as a union of 2 irreducible curves corresponds to a primary decomposition of its ideal. ( $\mathrm{wy}-x^{2}, y^{2}-\mathrm{xz}, \mathrm{wz}-\mathrm{xy}$ ) $\cap$ (wy $\left.-x^{2}, w^{2}, w x\right)$ The ideal is not radical: for example, $\left(y^{2}-\mathrm{xz}\right) x$ is not in the ideal but its cube is.

Example 30 How many point in projective space over a finite field? Method 1: projective space $=$ affine space + projective space at infinity. Method 2: Projective space $=$ affine space -point/ multiplicative group. Zeta function is $\exp \left(\sum\left(\right.\right.$ points over $\left.\left.\boldsymbol{F}_{q^{n}}\right) t^{n} / n\right)=1 /(1-t)(1-q t)\left(1-q^{2} t\right) \ldots\left(1-q^{\operatorname{dim}} t\right)$. Note relation to complex cohomology: Betti numbers of complex projective space can be read off from number of points over finite fields. Generalized by Weil conjectures.

Example 31 Is the product of 2 projective varieties projective? Analogue for affine varieties is easy: If $Y$ and $Z$ are given by ideals $I$ and $J$ in $k\left[x_{1}, \ldots x_{m}\right]$ and $k\left[y_{1}, \ldots y_{n}\right]$ then the product is given by the ideal generated by $I$ and $J$ in $k\left[x_{1}, \ldots x_{m}, y_{1}, \ldots y_{n}\right]$. This uses the fact that $A^{m} \times A^{n}=A^{m+n}$.

Analogue for projective space is FALSE: $P^{m} \times P^{n} \neq P^{m+n}$. The "obvious" map between them taking $\left(x_{0}: \ldots\right) \times\left(y_{0}: \ldots\right) \rightarrow\left(x_{0}: \ldots: y_{0}: \ldots\right)$ is simply not well defined as multiplying the $x$ 's by $\lambda$ gives a different image.

In fact over the complex numbers, $P^{1} \times P^{1}$ and $P^{2}$ are not even homeomorphic as topological spaces: look at 2nd cohomology. Other differences: any two curves in $P^{2}$ intersect (Bezout) but $P^{1} \times P^{1}$ has plenty of disjoint lines.

Instead, we can embed $P^{m} \times P^{n}$ as a projective variety inside $P^{m n+m+n}$ by mapping $\left(x_{0}: \ldots\right) \times\left(y_{0}: \ldots\right) \rightarrow\left(x_{0} y_{0}: \ldots: x_{i} y_{j}: \ldots\right)=\left(w_{00}: \ldots: w_{i j}: \ldots\right)$. (Segre embedding) In terms of lines in vector space, this is given by taking the tensor product of two lines in the tensor product of 2 vector spaces. What is
the ideal of its image? $w_{i j} w_{k l}=w_{i k} w_{j l}$. Check map is onto: Can assume that $w_{00}$ (say) is nonzero, so can assume it is 1 . Then $w_{k l}=w_{0 l} w_{k 0}=y_{l} x_{k}$, so map is onto.

For example, this identifies $P^{1} \times P^{1}$ with the nonsingular quadric $w z=x y$ in $P^{3}$, which therefore has 2 rulings. (Any 2 nonsingular quadrics in $P^{3}$ are isomorphic, and are ruled surfaces, sometimes used in architecture.)

Any nonsingular quadric in $P^{3}$ can be put in this form (pick norm 0 vectors); for example the sphere $x^{2}+y^{2}+z^{2}=1$ has 2 rulings by straight lines (over complex numbers)! $(x+i y)(x-i y)=(1-z)(1+z)$.

Example 32 Veronese surface is given by the points of the form ( $x^{2}$ : xy : $\mathrm{xz}: y^{2}: \mathrm{yz}: z^{2}$ ) in $P^{5}$. Embedding of projective plane into $P^{5}$. Equations: $w_{i j} w_{k l}=w_{i k} w_{j l}$ with $w_{i j}=w_{j i}$. Similar examples in higher dimensions.

Example 33 Example of a Grassmannian $G(m, n)$ is $m$ dimensional subspaces of $k^{m+n}$. $G(m, n)=G(n, m)$ (duality of vector spaces) and $G(1, n)$ is projective space, so first nontrivial case is $G(2,2)$, the planes on $k^{4}$ or the lines in $P^{3}$. Can we find a projective variety whose points correspond naturally to this space (and what does "naturally" mean?). Simplest nontrivial example of a HILBERT SCHEME: parametrizes subschemes of projective space, this this case of degree and dimension 1. (Note: lines in $A^{3}$ do not form an affine or a projective variety.)

We embed $G(2,2)$ in $P^{5}$. Suppose $a$ and $b$ span a line in $P^{3}$. Look at

$$
\left(\begin{array}{cccc}
a_{0} & a_{1} & a_{2} & a_{3} \\
b_{0} & b_{1} & b_{2} & b_{3}
\end{array}\right)
$$

Put $s_{i j}=$ determinant of columns $i$ and $j$. Then $\left(s_{i j}\right)$ is well defined in $P^{5}$ as changing 2 points of a line does not change rations of determinants. Is this onto? No! lines in $P^{3}$ form 4-dim space, so there must be a nontrivial relation between the $s_{i j}$. Relation is the Plucker relation

$$
s_{01} s_{23}-s_{02} s_{13}+s_{03} s_{12}=0
$$

(proof: each term occurs twice with opposite signs). Check map is onto. Suppose $s_{01}$ (say) is 1 . Then $s_{23}$ is determined by other $s$. So point it the image of

$$
\left(\begin{array}{llll}
1 & 0 & s_{12} & s_{13} \\
0 & 1 & s_{02} & s_{03}
\end{array}\right)
$$

So the set of lines in $P^{3}$ is isomorphic to a quadric in $P^{5}$.
We can use this to find cohomology of this quadric. The Grassmannian is the union of $\left(\begin{array}{llll}1 & 0 & * & * \\ 0 & 1 & * & *\end{array}\right)\left(\begin{array}{llll}1 & * & 0 & * \\ 0 & 0 & 1 & *\end{array}\right)$ etc, giving affine spaces of dimensions $0,1,2,2,3,4$, from which one can read off the cohomology, and the number of points over finite fields. (Differs from cohomology of $P^{4}$ )

Similar but more complicated argument shows that Grassmannians $G(m, n)$ are intersections of quadrics in some projective space of dimension $\binom{m+n}{m}-$ 1. Details: Pick $m$ vectors spanning subspace, which give a matrix of size $m \times(m+n)$. Then the $\binom{m+n}{m}$ determinants $p_{i_{1}, \ldots, i_{m}}$ of all $m \times m$ minors give projective space coordinates for a point of the Grassmannian. Find relations between them:

$$
0=\sum_{\lambda}(-1)^{\lambda} p_{i_{1}, \ldots, i_{m-1}, j_{\lambda}} \times p_{j_{1}, \ldots j_{\lambda-1}, j_{\lambda+1}, \ldots, j_{m+1}}
$$

because each monomial occurs twice, with opposite signs. (Enough to check for $m \times 2 m$ matrix.)

Now need to check this map from Grassmannian to projective space is ONTO. Image is covered by open affine subsets where some $p$ is nonzero. Suppose for example that $p_{1, \ldots, m}=1$. Then we can find a point of the Grassmannian with any given values of $p_{1, \ldots, r-1, r+1, \ldots, m, s}$, in other words with at least $m-1$ indices in $1, \ldots, m$, by choosing a matrix whose left columns form the identity matrix. But then the Plucker relations determine all the other $p$ 's using $p_{1, \ldots, m} p_{i_{1}, \ldots, i_{m}}=$ sum of terms with more indices in the set $1, \ldots, m$.

Grassmannians are particularly simple because they can be written as disjoint unions of affine spaces. They can also be given as quotients: $\mathrm{GL}_{m+n} /\left(\begin{array}{cc}* & * \\ 0 & *\end{array}\right)$, which shows that their dimension is $m n$. In particular the quotient of two AFFINE groups can be PROJECTIVE.

Used by Grothendieck in proof that components of Hilbert scheme are projective. Key idea: suppose a homogeneous ideal $I=I_{0}+I_{1}+\ldots$ of $k\left[x_{1}, \ldots\right]=$ $S_{0}+S_{1}+\ldots$ has the property that $\operatorname{dim}\left(I_{j}\right)=p(j)$ for $j$ large and some polynomial $p$ (more or less the Hilbert polynomial: see later). Fix $d$ sufficiently large, so that in particular $I_{d}$ generates all larger $I$ 's. Then the image of $I_{d}$ in $S_{d}$ is a point of the Grassmannian of $p(d)$-dimensional subspaces of a vector space of dimension $\operatorname{dim}\left(S_{d}\right)$. Relations defining the image of this subset: we have the image of the map $I_{d} \otimes S_{j} \rightarrow S_{d+j}$ is contained in $I_{d+j}$ so has rank at most $p(d+j)$. Recall that linear maps of rank at most something form a closed subset (a determinantal variety defined by lots of determinants being 0 ). The condition that all these maps have rank at most something gives the ideal defining the Hilbert scheme in the Grassmannian. (Actual construction more sophisticated, because of the technical problem that all ideals generated by $I_{d}$ of given dimension do not form a flat family. The restriction to ideals with given Hilbert polynomial is needed because these form a better behaved (flat) family.)

What does "natural" mean when we say that lines in $P^{3}$ is naturally isomorphic to this projective variety? Answer by Grothendieck: corresponding functors from commutative rings to sets are isomorphic;

Ring $R \rightarrow$ lines in projective space over $R$

Ring $R \rightarrow G(2,2)$ over $R$.
Ring $R \rightarrow R$-valued points of a projective variety in $P^{5}$
Isomorphic as functions: this means not only are $F(x), G(x)$ isomorphic as sets, but these isomorphisms commute with morphisms $x \rightarrow y$.

This requires working over more general commutative rings. More generally, any scheme determined up to isomorphism by its functor of points. Fundamental question: given a functor, such as "Picard group" "Hilbert scheme" "isomorphism classes of abelian varieties", is it represented by a scheme? Problem: it is tricky to define the correct functors from rings.

Elementary examples of Hilbert schemes include hypersurfaces in projective space, $n$ points on a line, and Grassmannians. These examples are misleadingly simple: in general Hilbert schemes seem to exhibit every imaginable sort of bad behavior of projective schemes (they can be singular at all points of a component for example).

Example 34 Hirzebruch surfaces. The quotient of $\left(A^{2}-0\right) \times\left(A^{2}-0\right)$ by $G_{m} \times$ $G_{m}$ acting as $(\lambda, \mu)(s, t, x, y)=\left(\lambda s, \lambda t, \mu x, \lambda^{-a} \mu y\right)$ for $a$ an integer. There is a map from $F$ to $P^{1}$ taking $(s, t, x, y) \rightarrow(s: t)$. The fiber at any point is isomorphic to $P^{1}$ so we get a fiber bundle, nontrivial unless $a=0$. Fiber bundle= "twisted product"; looks locally like a product, similar to a Moebius band.

Example 35 Scrolls. $F=F\left(a_{1}, \ldots, a_{n}\right)$ is the quotient of $\left(A^{2}-0\right) \times\left(A^{n}-0\right)$ by $G_{m} \times G_{m}$ acting as $(\lambda, \mu)\left(s, t, x_{1}, \ldots, x_{n}\right)=\left(\lambda s, \lambda t, \lambda^{-a_{1}} \mu x_{1}, \ldots, \lambda^{-a_{n}} \mu x_{n}\right)$. There is a map from $F$ to $P^{1}$ taking $\left(s, t, x_{1}, \ldots, x_{n}\right) \rightarrow(s: t)$. The fiber at any point is isomorphic to $P^{n-1}$ so we get a fiber bundle, usually nontrivial.

Assume all $a$ 's positive. Embedding of $F$ into projective space $P^{\sum\left(a_{i}+1\right)-1}$ by ratios of the $\sum\left(a_{i}+1\right)$ monomials (bihomogeneous polynomials) $s^{i} t^{a_{j}-i} x_{j}$. The image of each fiber is a linear subspace.

For $n=2$ these are the Hirzebruch surfaces.
Quasiprojective varieties are covered by open affine varieties. It is unnatural to assume all varieties should be embedded in projective space; this is rather like demanding that all differentiable manifolds should be subsets of Euclidean space. Weil defined abstract varieties as (roughly) things that can be covered by open affine varieties. Formal definition comes later using locally ringed space as special case of schemes. Work slightly informally. Weil originally introduced concept to construct abstract Jacobian varieties of curves over finite fields, though these turned out to be projective.

Toric varieties. Any rational polyhedral cone $C$ gives an affine variety, with coordinate ring the group ring of the DUAL cone. (Taking duals means maps of cones give maps of affine varieties.) Example: quadrant gives affine space, 0 gives a torus, cone generated by $(1,1)(1,-1)$ gives singular variety $k[x, y, z] /\left(z^{2}-x y\right)$. If we have a fan (collection of cones closed under taking faces, intersections) we get a collection of affine varieties that can be glued
together using inclusions of cones. Example: projective space, $P^{1} \times P^{1}$, weird examples with an infinite number of cones (not of finite type, not quasicompact).

All complete abstract varieties that are 1-dim or 2-dim and nonsingular are projective, but Hironaka gave example of a nonsingular complete 3 -dim variety that is not projective: see later. They don't seem to be of much interest, and Chow's lemma says they are covered by projective varieties by a map that is isomorphism over an open dense subset.

### 1.3 Morphisms

Background: recall definition of category. Examples: Sets, commutative rings, abelian groups, differentiable manifolds. Key point: when defining mathematical objects, ask what the morphisms are. In algebraic geometry there are 2 sorts of morphism: regular maps and birational maps.

Regular functions on an affine variety $=$ coordinate ring $k\left[x_{1}, \ldots\right] / I$.
Regular function $f$ on an open subset $U$ of an affine variety $V$ (quasiaffine variety) are functions that are regular at all points $p$ of $U$, meaning that $f=g / h$ in some neighborhood of $p$, where $h$ is nonzero in this neighborhood.

We should check that this is compatible with the definition for affine varieties! So suppose $V=U_{1} \cup U_{2} \cup \ldots$ and $f$ is a function on $V$ with $f=g_{i} / h_{i}$ on $U_{i}$ with $h_{i}$ nonvanishing on $U_{i}$. Here the $g$ 's and $h$ 's are in the coordinate ring of $V$, and we want to show that $f$ is too. We have

$$
1=a_{1} h_{1}+\ldots \bmod I
$$

because the $U_{i}$ cover $V$, so no max ideal contains all the $h$ 's and $I$. This suggests that

$$
f=a_{1} h_{1} f+\ldots \bmod I=a_{1} g_{1}+\ldots \bmod I
$$

So we DEFINE $f$ to be $a_{1} g_{1}+\ldots$ and check that $h_{i} f=a_{1} g_{1} h_{i}+\ldots=a_{1} g_{i} h_{1}+$ $\ldots \bmod I\left(\right.$ because $\left.h_{i} g_{j}=h_{j} g_{i} \bmod I\right)$, which is $g_{i} \bmod I$.

Similarly a function on a quasiprojective set (open subset of projective space) is called regular if it is locally regular at all points, or equivalently regular on all affine open subsets. This makes quasi projective varieties into RINGED SPACES: regular functions form a SHEAF. (Define sheaves.)

Example 36 Regular functions on $P^{1}=A^{1} \cup A^{1}$ given by $(f, g)$ with $f \in k\left[x_{0}\right]$, $g \in k\left[x_{1}\right]$, that coincide on $k\left[x, x^{-1}\right]$. So they are elements of $k\left[x, x^{-1}\right]$ that are polynomials in both $x$ and $x^{-1}$, so they are constants.

Definition 3 morphism $f: X \rightarrow Y$ is a continuous map such that the pullback of any regular function on any open $U \subset Y$ is regular on $f^{-1}(U) \subset X$. (Same as morphism of ringed spaces)

Warning: for general schemes this definition is WRONG: should use morphisms of LOCALLY ringed spaces, which for varieties happen to be same as morphisms of ringed spaces.

Examples of ringed spaces: manifolds with
top $=C^{0}, C^{1}, C^{2}, \ldots C^{\infty}, C^{\omega}$, algebraic structure
Morphisms in this $\rightarrow$ direction

## Floppy

 RigidLocal ring of a variety at a point $p$ is $\lim _{\rightarrow U \ni p}($ regular functions on $U)$. ROUGHLY functions defined near $p$. Check this is a local ring, with max ideal functions vanishing at $p$. Suppose $f \neq 0$ at $p$. Then $f=g / h$ with $g \neq 0$ at $p$, so $g \neq 0$ in some neighborhood, so $1 / f=h / g$ in this neighborhood is in the local ring.

So in fact a variety is a LOCALLY RINGED SPACE: this means stalks are LOCAL rings. .

Moreover morphisms of varieties are automatically morphisms of locally ringed spaces, meaning that pullback of something in a max ideal of a local ring is in max ideal, in other words pullback of function vanishing at $p$ vanishes at $f^{-1}(p)$. (Not always true for more general ringed spaces whose sections need not be functions on a space.)

Example 37 There is a morphism from $A^{1}$ to the cuspidal curve $y^{2}=x^{3}$ taking $t$ to $\left(t^{2}, t^{3}\right)$. Corresponding map off coordinate rings embeds $k\left[t^{2}, t^{3}\right] \subset k[t]$. This is a homeomorphism of the underlying topological spaces but is NOT an isomorphism of varieties.

Theorem 5 Suppose $Y$ is AFFINE. (False if not affine). Then morphisms from $X$ to $Y$ same as morphisms from $O(Y)$ to $O(X)$ where $O$ means regular functions.

Proof Suppose $\varphi \in \operatorname{Hom}(X, Y)$. Then $\varphi^{*}$ takes regular functions on $Y$ to regular functions on $X$ so we get an element of $\operatorname{Hom}(O(Y), O(X)$ (even if $Y$ is not affine). We need to construct an inverse $\operatorname{Hom}(O(Y), O(X) \Rightarrow \operatorname{Hom}(X, Y)$.

Suppose $h \in \operatorname{Hom}\left(O(Y), O(X)\right.$ where $O(Y)=k\left[x_{1}, \ldots\right] / I$. Define $\psi: X \rightarrow$ $Y$ as follows. $h\left(x_{i}\right) \in O(X)$, so if $p \in X$ then $h\left(x_{i}\right)(p) \in k$. Put

$$
\psi(p)=\left(h\left(x_{1}\right)(p), \ldots\right) \in k^{n}
$$

which defines a map $\psi: X \rightarrow k^{n}$. The image is in $Y$ as $h(I)=0$.
Check $\psi$ is a morphism. $x_{i} \circ \psi$ is regular on $X$ for each coordinate function $x_{i}$ on $Y$, so $f\left(x_{1}, \ldots\right) \circ \psi=f\left(x_{1} \circ \psi, \ldots\right)$ is regular for any regular $f$. Easy to check that map taking $h$ to $\psi$ is desired inverse map.

Corollary: Category of affine algebraic sets over algebraically closed fields $k$ is equivalent to the opposite (define this) of category of finitely generated reduced $k$-algebras. For example, (categorical) product of algebraic varieties corresponds to coproduct $=$ tensor product of the coordinate rings. Example: $A^{1} \times A^{2}=A^{3}$ and $k\left[x_{1}\right] \otimes k\left[x_{2}, x_{3}\right]=k\left[x_{1}, x_{2}, x_{3}\right]$. Warning: this fails over non-perfect fields, because the tensor product of two reduced finitely generated algebras over a field need not be reduced. An example is given by taking a (nonperfect) field $k$ of characteristic $p>0$ such as $F_{p}(t)$ and forming the inseparable extension $K=k\left[t^{1 / p}\right]$ where $t$ has no $p$ th root in $k$. Then $K$ is a field so is reduced, but $K \otimes_{k} K$ has nilpotent elements.

Example 38 Algebraic group $G \times G \rightarrow G$.
$G_{a}:(x, y) \rightarrow x+y$ This corresponds to a map $k[x] \otimes k[y] \leftarrow k[z]$ taking $z$ to $x+y$.
$G_{m}:(x, y) \rightarrow x y$ This corresponds to a map $k\left[x, x^{-1}\right] \otimes k\left[y, y^{-1}\right] \leftarrow k\left[z, z^{-1}\right]$ taking $z$ to $x y$.

$$
\mathrm{GL}_{2}(k):\left(\begin{array}{cc}
a_{1} & b_{1} \\
c_{1} & d_{1}
\end{array}\right)\left(\begin{array}{cc}
a_{2} & b_{2} \\
c_{2} & d_{2}
\end{array}\right)=\left(\begin{array}{cc}
a_{1} a_{2}+b_{1} c_{2} & a_{1} b_{2}+b_{1} d_{2} \\
c_{1} a_{2}+d_{1} c_{2} & c_{1} b_{2+} d_{1} d_{2}
\end{array}\right) \text { Coor- }
$$

dinate ring $R$ is $k[a, b, c, d] /(a d-b c-1)$. Corresponding map from $\Delta: R \rightarrow R \otimes R$ takes $a$ to $a_{1} a_{2}+b_{1} c_{2}$, etc. Exercise: describe homomorphism from $R$ to $R$ corresponding to INVERSE of group.
(Coordinate rings of affine algebraic groups are commutative HOPF ALGEBRAS.)

Example 39 We check that the twisted cubic is isomorphic to $P^{1}$. There is a natural map from $P^{1}$ to the twisted cubic taking $(s: t)$ to $\left(s^{3}: s^{2} t: s t^{2}: t^{3}\right)$ and this is isomorphism of underlying top spaces, but this is NOT enough to prove it is an isomorphism of varieties. We need to construct a morphism in the other direction. The twisted cubic is covered by 2 affine subsets $w \neq 0$ and $z \neq 0$ so we can define the inverse morphism on each of these two subsets and check it is the same on their intersection.
$w \neq 0:(w: x: y: z) \rightarrow(w: x)$
$z \neq 0:(w: x: y: z) \rightarrow(y: z)$
As $w z=x y$ these coincide on $w \neq 0 \wedge z \neq 0$.
Note that the corresponding graded rings $k[s, t]$ and $k[w, x, y, z] /\left(\mathrm{wz}-\mathrm{xy}, \mathrm{wx}-x^{2}, \mathrm{xz}-y^{2}\right)$ are NOT isomorphic!

Example $40 A^{1}-0$ is isomorphic to the affine variety xy $=1$. However the quasiaffine variety $A^{2}-(0,0)$ is not isomorphic to ANY affine variety. To see this calculate its coordinate ring. Cover it by the 2 open affine subsets $x \neq 0$ and $y \neq 0$. Then the Coordinate ring consists of pairs in $k\left[x, x^{-1}, y\right] \times k\left[x, y, y^{-1}\right]$ with same image in coordinate ring $k\left[x, x^{-1}, y, y^{-1}\right]$ of the intersection. This is just $k[x, y]$. So maps from $A^{2}-(0,0)$ to affine varieties are "same as" maps from $A^{2}$ to affine varieties, so it cannot be affine as the natural map to $A^{2}$ is not an isomorphism.

Example 41 (Suggested by Arend Bayer on mathoverflow). The group $\mathrm{GL}_{2}(k)$ acts in the obvious way on $P^{1}$. If we fix a point of $P^{1}$ we get a morphism of an affine variety onto a projective variety with affine fibers. In particular the quotient of 2 affine groups need not be affine, and a fiber bundle with affine fibers over a projective variety can be affine.

Example 42 Products of affine varieties. Recall product of objects of any category. Product is unique up to unique isomorphism. (For example, there are several ways to define the ordered pair in set theory, such as $\{a,\{a, b\}\}$ or $\{\{\mathrm{a}, 1\},\{\mathrm{b}, 2\}\}$ or $\{\{a\},\{a, b\}\}$, but the all give canonically isomorphic products of sets.) Product of affine varieties corresponds to coproduct=tensor
product of commutative rings. Notice that products and coproducts of objects depend on the category. For example, the product of affine varieties does NOT have the same topology as their product as topological spaces. Another random example: the coproduct of 2 commutative rings is different in the categories of commutative rings and non-commutative rings.

Example 43 Products of projective varieties. We want to check that the Segre embedding gives the product $P^{m} \times P^{n}$, which is unique up to canonical isomorphism. The proof is essentially trivial, but involves some bookkeeping and unwinding definitions. We need to give maps from the Segre embedding to $P^{m}$ and $P^{n}$ and then check it has the universal property. Recall the fundamental technique: cover by open affine subsets. Element of Segre embedding is $\left(z_{00}: \ldots: z_{\mathrm{mn}}\right)$ Define map to $P^{m}$ on (say) the open set with $z_{00} \neq 0$ as $\left(z_{00}: z_{10}: \ldots: z_{m 0}\right)$. On the open set with (say) $z_{01} \neq 0$ the map is given by $\left(z_{01}: z_{11}: \ldots: z_{m 1}\right)$. Check these two maps are same on the intersection: this follows from the relations $z_{\mathrm{ij}} z_{\mathrm{kl}}=z_{\mathrm{il}} z_{\mathrm{jk}}$. So we have a well defined morphism to $P^{m}$.

Now we have to check the universal property, so suppose we have a variety $V$ mapping to $P^{m}$ and $P^{n}$. The first problem is that it is not that easy to describe regular maps from $V$ to projective space. We bypass this by covering $V$ with open affine sets such that each has image in one of the standard open affine sets covering projective space, say $z_{0} \neq 0$. So first assume $V$ is affine. Then a morphism to the open affine subset $z_{0} \neq 0$ of $P^{m}$ is given by regular functions $\left(f_{0}=1: f_{1}: \ldots: f_{m}\right)$ on $V$. Similarly a morphism to $P^{n}$ is given by $\left(g_{0}=1: g_{1}: \ldots: g_{n}\right)$. Then we can define a morphism to the Segre embedding by $\left(f_{0} g_{0}: \ldots: f_{m} g_{n}\right)$ and check this has required properties (image is in Segre embedding, etc.) For general $V$, the morphisms on sets of an open affine cover are compatible on intersections by the uniqueness property of the product, so they fit together to give a morphism to the image of the Segre embedding.

The Segre embedding is really a combination of 2 different operations: a product of projective spaces as an abstract variety, together with an embedding of this abstract variety into projective space. The embedding into projective space is really irrelevant, and it is easier to define the abstract product of varieties and forget about projective embeddings: this is what we will do for products of schemes.

Example 44 Automorphisms of affine space. For $A^{1}$ these correspond to automorphisms of $k[x]$, which just map $x \rightarrow \mathrm{ax}+b$ for nonzero $a$, so we get a 2-dimensional nonabelian group. For $A^{n}$ with $n>1$ the automorphism group is MUCH larger. We can still map $x \rightarrow \mathrm{Ax}+B$ for matrices $A, B$ with $A, B$ invertible, but there are many other automorphisms not in this subgroup: for example $x \rightarrow x, y \rightarrow y+p(x)$ for any polynomial $p$, giving an infinite dimensional abelian subgroup. Suppose we have a morphism of affine space given by $x_{i} \rightarrow f_{i}\left(x_{1}, \ldots, x_{n}\right)$. Look at the Jacobian $\partial f_{i} / \partial x_{j}$. Then Jacobian of FG is jacobian of $F$ times Jacobian of $G$, so the jacobian of an automorphism is an
invertible polynomial, in other words a nonzero constant. Jacobian conjecture: does the converse hold? (There have been many incorrect proposed solutions).

Example 45 Morphisms of the projective line $P^{1}$ to itself. Any morphism restricts to a map from a (possibly empty) open set of $A^{1}$ to $A^{1}$, which is either empty or a rational function on $A^{1}$. Conversely rational functions on $A^{1}$ extend to morphisms of $P^{1}$, so the morphisms of $P^{1}$ correspond to rational functions together with $\infty$. The ones with inverses are just the ones of degree 1, corresponding to the group $\mathrm{PGL}_{2}(k)$. The automorphisms of the affine line and the projective line over the complex numbers are the same as the automorphisms of the complex plane and the complex sphere in complex analysis, and morphisms of the projective complex line to itself are the same as morphisms from the complex sphere to itself. (However morphisms from the affine line to itself are not the same as morphisms from the complex plane to itself.) This is a special case of Serre's GAGA: roughly speaking, in the projective setting analytic things tend to be algebraic.

Example 46 Consider the image of the morphism from $A^{2} \rightarrow A^{2}$ taking $(x, y) \rightarrow(x, x y)$. The image is plane $-y$ axis + origin so is not affine or locally closed.

Example 47 Ax-Grothendieck theorem. Suppose $f$ is an injective morphism from a variety to itself over an algebraically closed field, Then $f$ is surjective. (This is false over $\boldsymbol{Q}$ : consider $x \rightarrow x^{3}$.) Proof:

1. Trivial over finite fields: any injective map on a finite set is surjective.
2. Trivial over algebraic extensions of finite fields (such as the algebraic closure): take the finite field generated by the coefficients of the equations defining the variety, the $\operatorname{map} f$, and a point in the variety.
3. Now use fact that a 1 st order statement is true for algebraically closed fields of characteristic 0 if and only if it is true over algebraically closed fields of large prime characteristic.

This is related to the Lefschetz principal. Suppose $S$ is a statement in the first order language of fields. Then the following are equivalent:

1. $S$ is true in the complex numbers
2. $S$ is true in some algebraically closed field of characteristic 0
3. $S$ is true for some algebraically closed fields of arbitrarily large characteristic.
4. $S$ is true for all algebraically closed fields of sufficiently large characteristic

The key point is that the theory of algebraically closed fields of given characteristic is complete, which follows from the fact that it is categorical in uncountable cardinals. So any two algebraically closed fields of the same characteristic are
indistinguishable using first order statements. Characteristic 0 is defined by the statements $2 \neq 0,3 \neq 0, \ldots$ and any proof uses only a finite number of these, so applies to all algebraically closed fields of sufficiently large characteristic.

This gives two powerful methods for proving things for all algebraically closed fields in characteristic 0 :

Use analysis, Riemannian geometry, hodge theory etc. Then apply Lefschetz principle.

Prove for algebraic closures of finite fields, using counting arguments, Weil conjectures, Frobenius endomorphism, etc. (Famous example: Mori's bend and break argument.)

### 1.4 Rational maps

Suppose $Y$ is affine variety. As $Y$ is irreducible we can take quotient field $K(Y)$ of integral domain $O(Y)$. Elements are called RATIONAL FUNCTIONS on $Y$. No analogue for smooth manifolds: characteristic of algebraic geom. Analogous to meromorphic functions on Riemann surfaces/complex manifolds.

Definition fails for projective varieties as $O(Y)$ is too small. So instead we define the ring of rational functions to be
(regular functions on dense open set of $Y$ )/(equivalent if equal on intersection).
(Note that any 2 dense open sets have dense intersection, and if $Y$ is irreducible all nonempty open sets are dense, and in this case the rational functions form a field as the points where a nonzero function is nonzero is dense.)

So $K(Y)=\lim _{\rightarrow U}$ dense open $O(U)$.
Similarly define a rational map from $X$ to $Y$ to be given by a morphism on a dense open set, modulo obvious equivalence relation. So rational functions are same as rational maps to $A^{1}$. Rational maps do NOT form morphisms of a category: composition need not be defined, as the image of a rational map may have dense open complement! To fix this define a rational map to be DOMINANT if its image of some dense open set is dense. Two varieties are called BIRATIONAL if there is an invertible rational map from one to the other. This is a cruder equivalence relation than isomorphism. (For smooth metrizable manifolds, any 2 of same dimension are "birational".)

Example 48 The varieties $A^{1}, P^{1}, x y=1, x^{3}=y^{2}$ are all birational, but no 2 are isomorphic. Similarly $P^{1} \times P^{1}, P^{2}, A^{2}, A^{2}-(0,0)$

Example 49 We show that that affine line is not birational to the elliptic curve $x^{3}+y^{3}=1$. and more generally that there is no dominant map from $A^{1}$ to this curve. Algebraic proof: Suppose $x(t)^{3}+y(t)^{3}=1$ for rational functions $x$, $y$ of $t$. Clearing denominators we get $f(t)^{3}+g(t)^{3}=h(t)^{3}$. Factoring we get $(f+g)(f+\omega g)\left(f+\omega^{2} g\right)=h^{3}$. As polynomials form a UFD and every unit is a cube, the three terms on the left are all cubes, say $f+\omega^{k} g=h_{k}^{3}$. Eliminating $f$ and $g$ from these 3 equations gives a linear relation between the $h_{k}^{3}$, which have
smaller degrees than $f, g, h$, so by induction on the degree there is no solution in positive degree polynomials. (Same proof works for any exponent at least 3 . Note that over the rationals, zero degree is FAR harder than positive degree!) Shorter proof using more algebraic geom: there is no non-constant map from a curve to a curve of higher genus.

Example 50 We show the affine line is not birational to some elliptic curves $y^{2}=4 x^{3}-g_{2} x-g_{3}$ using complex analysis/topology. Use Weierstrass $\wp$ to construct an isomorphism from $\boldsymbol{C} / \Lambda$ to the curve. Recall that

$$
\wp(z)=\sum_{\lambda \in L} \frac{1}{(z-\lambda)^{2}}
$$

which is doubly periodic, except that this does not converge so we regularize it by

$$
\wp(z)=\frac{1}{z^{2}}+\sum_{\lambda \in L-0} \frac{1}{(z-\lambda)^{2}}-\frac{1}{\lambda^{2}}
$$

This is not clearly doubly periodic, but its derivative is as the series then converges. So $\wp$ is periodic up to "constants of integration", and the fact that $\wp$ is even implies that these constants all vanish.

Its Laurent expansion at 0 is $z^{-2}+O\left(z^{2}\right)$ so $\wp^{\prime}(z)^{3}=4 z^{-6}+(?) z^{-2}+(?) z^{0}+$ ... so we get

$$
\wp^{\prime}(z)^{2}=4 \wp(z)^{3}-g_{2} \wp(z)-g_{3}
$$

because both sides are doubly periodic with no poles and vanishing constant term. So the map taking $z$ to $\left(\wp(z), \wp^{\prime}(z)\right)$ maps $\boldsymbol{C} / \Lambda$ to the projective completion of the elliptic curve $y^{2}=4 x^{3}-g_{2} x-g_{3}$.

Reason for name elliptic curve/function etc: we have

$$
z=\int^{\wp} \frac{d \wp}{\sqrt{4 \wp(z)^{3}-g_{2} \wp(z)-g_{3}}}
$$

and the integral on the right is an elliptic integral related to finding the arc length of an ellipse.

Then $S^{2}$-finite number of points is never homeomorphic to $\boldsymbol{C} / \Lambda$-finite number of points so $P^{1}$ cannot be birational to $y^{2}=4 x^{3}-g_{2} x-g_{3}$. The group law on the elliptic curve is obvious in the analytic setting as it is a quotient of two abelian groups.

There is a similar construction for singly periodic functions:

$$
\sum_{\lambda \in Z} \frac{1}{z-\lambda}=\pi \cot (\pi z)
$$

if the left hand side is regularized in a suitable way. This is the logarithmic derivaative of Euler's product formuls for the sine function, and there is an analogue of this product formula for the Weierstrass function, leading to the theory of theta functions.

Example 51 Cubic surfaces are usually rational. Informal argument: Take 6 points in general position in $P^{2}$ so that the space of cubics vanishing on all of them is $10-6=4$ dimensional, basis $f_{1}, f_{2}, f_{3}, f_{4}$. This gives a map from $P^{2}-6$ points to $P^{3}$; image is some hypersurface. To find its degree, look at number of intersection points of image with some line, say $f_{1}=f_{2}=0$. There are $3 \times 3=9$ points of intersection of these 2 cubics, consisting of the 6 points we chose +3 others. The images of these 3 other points are the 3 points of intersection of the surface with the line, so degree $=3$. Now count dimensions: space of cubic surfaces has dimension $20-1=19$ (projective space). Dim of space of 6 points $=6 \times 2=12$. Subtract automorphisms of $P^{2}(\operatorname{dim} 8)$ and add $\operatorname{dim} \operatorname{aut}\left(P^{3}\right)=15$ to get $\operatorname{dim} 12-8+15=19$. So spaces have same dimension, so that most cubic surfaces arise in this way.

27 lines on cubic surface come from: 6 blown up points +15 lines through 2 points +6 quadrics through 5 points.

Argument is rather sloppy (typical of old Italian style algebraic geom): for example, what does "general position" mean for the 6 points? A. No 3 on line, no 6 on conic, but this takes more work.

A variety is called unirational if it is finitely covered by a rational variety. These are hard to distinguish from rational varieties. In 1 and 2 dimensions unirational implies rational (Luroth, Castelnuovo) and for many years it was an open problem to find any examples of unirational varieties that are not rational. Clemens and Griffiths showed that a cubic three-fold is unirational but in general not a rational variety

### 1.4.1 Blowing up

Blowup of $A^{n}(0,0, . .0)$ at a point means replace point by a copy of projective space. Given by points $\left(x_{1}, \ldots, x_{n}\right) \times\left(y_{1}: \ldots: y_{n}\right) \in A^{n} \times P^{n-1}$ with $x_{i} y_{j}=$ $x_{j} y_{i}$. Projection to $A^{n}$ is an isomorphism except at the origin, where inverse image is $P^{n-1}$. It is proper as it is a closed subset of $A^{n} \times P^{n-1}$.
$P^{n-1}$ is covered by affine spaces such as $y_{1} \neq 0$. On this open subset we can put $y_{1}=1$ so $x_{i}=y_{i} x_{1}$ : we get new coordinates $x_{1}, y_{2}, \ldots, y_{n}$. So blowing up means roughly divide $x_{2}, \ldots, x_{n}$ by $x_{1}$, and same for other coordinates.

Example: $y^{2}=x^{3}$. Blowup: put $y=x t$ so get $x^{2} t^{2}=x^{3}$. Get $x=0$, $x=t^{2}$ as 2 components. $x=0$ is the exceptional curve. Can also put $x=s y$ so we get $y^{2}=y^{3} s^{3}$ to get exceptional curve $y=0$ and a curve $1=y s$. Note result is NONSINGULAR (see next section...) so blowing up has resolved the singularity.

Example: $x^{2}+y^{2}=z^{2}$ Conical singularity DIAGRAM. Blowup: $x=z s, y=$ $t z$ so we get $z^{2}\left(s^{2}+t^{2}-1\right)=0$ : Cylinder.

Example: $y^{8}=x^{5}$ Blowup $x=y t$ gives $y^{3}=t^{5}$. Blowup using $y=s t$ gives $s^{3}=t^{2}$. Third blowup makes it nonsingular.

Example: $x y^{2}=z^{2}$ (Pinch point or Whitney umbrella.) Blowing up along the "worst" singularity at the origin just reproduces the same singularity. Instead blow up along line $y=z=0 .(x, y, z) \times(s: t) \in A^{3} \times P^{1}$ with yt $=\mathrm{sz}$.

Take (say) $s=1$ to get $z=t y$, so $\left(x-t^{2}\right) y^{2}=0$. This shows one cannot resolve singularities by repeatedly blowing up along subvariety of "worst" singularities, at least not using naive definitions.

Example: Blowing up real affine plane at a point gives real projective plane minus a point, as a line bundle over projective line $=$ circle, in other words a Moebius band without its boundary. Note that blowing up can turn an orientable manifold into a non-orientable one.

More generally can blow up along points or subvarieties or sheaves of ideals or sheaves of graded algebras. (Example: blowing up a point along the sheaf of graded algebras $k\left[x_{0}, \ldots\right]$ gives projective space.) Meaning is roughly replace each point by some projective variety, such as projective space of the normal space at a point, or the projective variety of a graded algebra. Blowup pulls apart the different normal vectors. Hironaka used repeated blowups to construct a PROPER birational map from a nonsingular variety to a char 0 variety. Idea is roughly that a singular variety is a projection of a nonsingular variety in a higher dimensional space.

Blowup over ideal: map $\left(x_{1}, \ldots, x_{m}\right) \rightarrow\left(x_{1}, \ldots, x_{m}\right) \times\left(g_{1}: \ldots: g_{n}\right) \in$ $A^{m} \times P^{n-1}$ where the $g$ 's are some polynomials. Defined for points not in the variety defined by the ideal $\left(g_{1}, \ldots\right)$. Take Zariski closure of points of $X$ not in this set. Up to isomorphism this only depends on the ideal generated by the $g$ 's and gives the blowup with center the ideal (or subscheme). Special case $g_{i}=x_{i}$ is just blowup at origin.

Example: Blow up affine plane along ideal $\left(x, y^{2}\right)$ has coordinate rings $k\left[x, y, y^{2} / x\right]$ and $k\left[x, y, x / y^{2}\right]$. The second is a polynomial ring, but the first is singular $y^{2}=x z$ (conical singularity). Similarly blowing up along the ideal $\left(x^{2}, y^{2}\right)$ produces a pinch point. Blowing up can be used to resolve singularities, but can also create new singularities. (This is why when blowing up along a subvariety one tries to use nonsingular subvarieties.) Blowing up along nonreduced subscheme like this is not always bad: Hironaka's theorem implies that in char 0 one can resolve any singularity by blowing up along some possibly nonreduced subscheme. Open problem: find a direct construction of such a subscheme. Blowing up along nonreduced subschemes seems a powerful and dangerous tool, but is not well understood.

### 1.4.2 The Atiyah flop

Flop: special sort of birational map used in classification of varieties of dim at least 3. First example found by Atiyah in 1958 as follows. Look at $x y=z t$ in $A^{4}$, a 3 -dim variety with a sing at origin. Blow up at 0 . Exceptional variety is $X Y=Z T$ in $P^{3}$. This resolves singularity as along (say) $X=1$ it looks like $Y=Z T$ in coordinates $x, Y, Z, T$. Exceptional variety is isomorphic to $P^{1} \times P^{1}$ which can be projected onto $P^{1}$ in 2 ways. So we can "half blow up" singularity along line $y=t=0$ by mapping it to $A^{4} \times P^{1}$ as $x y=z t, x Z=z X, t Z=y X$. If (say) $X=1$ this becomes $y=t Z, z=x Z, x y=z t$, which reduces to affine 3 -space so is nonsingular. We can also half blow it up to get $x y=z t, x T=t X$, $z T=y X$. The rational map between these two spaces is the Atiyah flop: it is
a birational map between nonsingular 3 -folds that changes a codimension $2 P^{1}$ to a different $P^{1}$ and is otherwise an isomorphism. This also shows that in 3 dims there is in general no nonsingular "minimal" resolution (though there is in $\operatorname{dim} ; 3$ ). To find a minimal model in dimension 3 , allow mild singularities, called terminal singularities.

### 1.5 Nonsingular varieties

### 1.5.1 Tangent spaces

Tangent space of $V$ with ideal generated by $f_{i}$ at $(0, \ldots, 0)$ given by vanishing of LINEAR parts of $f_{i}$. Origin is called a singular point if tangent space has "wrong" dimension $>\operatorname{dim}(\mathrm{V})$. For other points change variable to make point at origin. Dim of tangent space given by $n-\operatorname{rank}\left(\partial f_{i} / \partial x_{j}\right)$

Example: $f(x, y)$ nonsingular at 0 if some linear term nonzero. Converse true if $f$ REDUCED but not in general.

Example: For hypersurface, singular if $f=\partial f / \partial x_{i}=0$. Example: $y^{2}=$ $x^{3}+x^{2}-x-1$ singular at $(-1,0)$.

Set of singular points is CLOSED. Proof: Condition for a matrix to have rank $<n-\operatorname{dim}(V)$ is a closed subset of all matrices. (Determinantal variety!)

Set of nonsingular points is NONEMPTY.
Apparent counter-example: $x^{3}+y^{3}=1$. nonsingular at all points except in char 3 where ALL points are singular! This does not contradict result that nonsingular points are dense, because in char $3 x^{3}+y^{3}-1=(x+y-1)^{3}$. Schemes CAN be singular at all points.

Proof: Reduce to case of hypersurface $f=0$, as every variety is birational to a hypersurface. If all points are singular then all derivatives of $f$ vanish whenever $f$ vanishes so are divisible by $f$. As $f$ is irreducible and derivatives have lower degree, all derivatives vanish. This does NOT in general imply that $f$ is constant! But does imply that $f$ is $p$ 'th power of some thing, so as $f$ is irreducible it must be constant, contradiction.

As nonsingular points are open and nonempty, they are DENSE.
At nonsingular points variety is smooth manifold over reals or complex numbers. (Warning: $y^{2}=x^{3}$ is a topological manifold even though it is singular at $(0,0))$.

Problem: Tangent space seems to depend on embedding of variety into affine space. Need to find INTRINSIC definition of tangent space. A: It is given by the Zariski tangent space $\left(\mathfrak{m} / \mathfrak{m}^{2}\right)^{*}$ where $\mathfrak{m}$ is the max ideal of the local ring, so that $\left(\mathfrak{m} / \mathfrak{m}^{2}\right)$ is a vector space over $k$. To see this it is enough to check it for the point $(0, \ldots, 0)$ for a variety whose ideal is generated by the polynomials $f_{i}$. We observe that $\left(\mathfrak{m} / \mathfrak{m}^{2}\right)$ is $\left(x_{1}, \ldots, x_{n}\right) /\left(\right.$ terms of degree $\left.\geqslant 2, f_{i}\right)$ which can be identified with the "cotangent space" (vector space with basis $\left.x_{1}, \ldots, x_{n}\right) /$ (linear partsof $f_{i}$ ) whose dual is just the subspace of $k^{n}$ on which the linear parts of the $f_{i}$ vanish, in other words the tangent space.

Another viewpoint: Zariski tangent space of local ring over a field $k$ equal to the residue field $=$ homomorphisms to $k[\varepsilon] /\left(\varepsilon^{2}\right)$. Geometrically this is maps
from $\operatorname{Spec}\left(k[\varepsilon] /\left(\varepsilon^{2}\right)\right)$ which is a sort of point with an infinitesimal line coming from it; an analogue of a "short smooth curve" in differential manifolds. (Note use of non-reduced scheme.) This analogue fails for tangent space of Spec(p-adic numbers).

Yet another viewpoint: consider tangent and cotangent vector fields on a differentiable manifold. These are modules over the ring $R$ of smooth functions, and there is a linear derivation $d$ from $R$ to cotangent vector fields. Define the module $M$ of cotangent fields over a ring to be the image of the universal derivation (generators $d f$, relations $d(f+g)=d f+d g, d(f g)=f d g+g d f$ (Leib$n i z)$ ). If we do this for the coordinate ring of an affine variety we get module of cotangent fields. Example: for $k\left[x_{1}, \ldots x_{n}\right]$ this is a free module with basis $d x_{1}, \ldots d x_{n}$. Module of tangent vector fields $=$ dual $\operatorname{Hom}(M, R)$. Cotangent space of point can be reconstructed by (localizing at that point and) taking quotient by maximal ideal.

Direct construction of cotangent module: let $I$ be kernel of $R \otimes R \rightarrow R$ and put $M=I / I^{2}$ (with $R$ acting on left component), $d r=1 \otimes r-r \otimes 1$. Check $d$ is a derivation: $1 \otimes a b-b a \otimes 1=a(1 \otimes b-b \otimes 1)+b(1 \otimes a-a \otimes 1)+(1 \otimes a-a \otimes 1)(1 \otimes$ $b-b \otimes 1)$. Check universal property: Suppose we have a derivation $d$ to some module $M$. Define $f: R \otimes R \rightarrow M$ by $f(a \otimes b)=a d b$. Check this vanishes on $I^{2}:$ if $\sum s_{i} \otimes t_{i} \in I, \sum u_{j} \otimes v_{j} \in I \in I$, then $\sum s_{i} t_{i}=0, \sum u_{j} v_{j}=0$ so $f\left(\left(\sum s_{i} \otimes\right.\right.$ $\left.\left.t_{i}\right)\left(\sum u_{j} \otimes v_{j}\right)\right)=\sum s_{i} u_{j} d\left(t_{i} v_{j}\right)=\sum s_{i} d t_{i} \sum u_{j} v_{j}+\sum s_{i} t_{i} \sum u_{j} d v_{j}=0$ so $f$ vanishes on $I^{2}$ so gives a map from $I / I^{2}$ to $M$. This construction will later be used for constructing the cotangent sheaf of a scheme. Geometric interpretation: tangent space something like infinitesimal neighborhood of diagonal $V$ in $V \times V$. (Compare with tangent microbundle of a topological space.)

Definition: A local ring is called REGULAR if its dimension is $\operatorname{dim}\left(\mathfrak{m} / \mathfrak{m}^{2}\right)$ and a variety is called NONSINGULAR at a point if the local ring is regular.

### 1.5.2 Example: resolution of $E_{8} \mathbf{D u}$ Val singularity $x^{2}+y^{3}+z^{5}=0$

A du Val singularity, also called simple surface singularity, Kleinian singularity, or rational double point or canonical singularity in $\operatorname{dim} 2$, is a quotient of $\boldsymbol{C}^{2}$ by action of finite group, such as binary icosahedral group of order 120 (inverse image of $A_{5}$ in unit quaternions) (Klein). Ring of invariant generated by 3 elements $x, y, z$ satisfying the relation above. For example, for cyclic group of order $n$ acting as $X \rightarrow \zeta X, Y \rightarrow \zeta^{-1} Y$, ring of invariant is generated by $x=$ $X^{n}, z=\mathrm{XY}, y=Y^{n}$ satisfying the relation $z^{n}=x y=(x+y)^{2} / 4-(x-y)^{2} / 4$, so is of type $A_{n-1}$.

$$
\begin{array}{rll}
\operatorname{cyclic} A_{n} & : & x^{2}+y^{2}+z^{n+1}=0 \\
\text { dihedral } D_{n} & : & x^{2}+z y^{2}+z^{n-1}=0 \\
\text { tetrahedral } E_{6} & : x^{2}+y^{3}+z^{4}=0 \\
\text { octahedral } E_{7} & : x^{2}+y^{3}+y z^{3}=0 \\
\text { icosahedral } E_{8} & : x^{2}+y^{3}+z^{5}=0
\end{array}
$$

Assume char $=0$. Only singularity is at $(0,0,0)$.

Blow up using ( $x_{1}: y_{1}: z_{1}$ ) as coordinates for $P^{2}$. Cover $P^{2}$ by 3 copies of $A^{2}$ and check for singularities:

- $x_{1}=1: x^{2}+y_{1}^{3} x^{3}+z_{1}^{5} x^{5}=0 \rightarrow 1+y_{1}^{3} x+z_{1}^{5} x^{3}=0$ Sing if also $x=0$, not possible.
- $y_{1}=1: x_{1}^{2} y^{2}+y^{3}+z_{1}^{5} y^{5}=0 \rightarrow x_{1}^{2}+y+z_{1}^{5} y^{3}=0$ Sing if also $2 x_{1}=0$, $5 z_{1}^{4} y^{3}=0,1+3 z_{1}^{5} y^{2}=0$, no possible.
- $z_{1}=1: x_{1}^{2} z^{2}+y_{1}^{3} z^{3}+z^{5}=0 \rightarrow x_{1}^{2}+y_{1}^{3} z+z^{3}=0$. Singular if also $2 x_{1}=0$, $3 y_{1}^{2}=0, y_{1}^{3}+3 z^{2}=0$, so singular if all coordinates 0 .

So we now have to resolve singularity of $x_{1}^{2}+y_{1}^{3} z+z^{3}=0$ at origin.
As before, blow up introducing coordinates $\left(x_{2}: y_{2}: z_{2}\right)$ with $x_{2} z=z_{2} x_{1}$, etc.

- $x_{2}=1$ : Nonsingular
- $y_{2}=1: x_{2}^{2} y_{1}^{2}+y_{1}^{4} z_{2}+y_{1}^{3} z_{2}^{3}=0 \rightarrow x_{2}^{2}+y_{1}^{2} z_{2}+y_{1} z_{2}^{3}=0$ Sing at $(0,0,0)$
- $z_{2}=1: x_{2}^{2} z^{2}+y_{2}^{3} z^{4}+z^{3}=0 \rightarrow x_{2}^{2}+y_{2}^{3} z^{2}+z=0$ Nonsingular.

So we now have to resolve singularity of $x_{2}^{2}+y_{1}^{2} z_{2}+y_{1} z_{2}^{3}=0$ at origin. Not really clear what we have gained as this seems just as complicated as what we started with! This shows that measures of the complexity of a singularity have to detect quite subtle properties.

Introduce $\left(x_{3}: y_{3}: z_{3}\right)$.

- $x_{3}=1$ : Nonsingular
- $y_{3}=1: \quad x_{3}^{2} y_{1}^{2}+y_{1}^{3} z_{3}+y_{1}^{4} z_{3}^{3}=0 \rightarrow x_{3}^{2}+y_{1} z_{3}+y_{1}^{2} z_{3}^{3}=0$ Sing if also $2 x_{3}=0, z_{3}+2 y_{1} z_{3}^{3}=0, y_{1}+3 y_{1}^{2} z_{3}^{2}=0$ which forces all to be 0 .
- $z_{3}=1: x_{3}^{2}+y_{3}^{2} z_{2}+y_{3} z_{2}^{2}=0$ so also $2 x_{3}=0,2 y_{3} z_{2}+z_{2}^{2}=0, y_{3}^{2}+2 y_{3} z_{2}=0$ so sing is at $(0,0,0)$
So there are TWO singularities at $\left(x_{3}: y_{3}: z_{3}\right)=(0: 1: 0),(0: 0: 1)$.
First look at the singularity $x_{3}^{2}+y_{1} z_{3}+y_{1}^{2} z_{3}^{3}=0$ at $\left(x_{3}: y_{3}: z_{3}\right)=(0: 1: 0)$. Blowup introducing ( $x_{4}: y_{4}: z_{4}$ ).
- $x_{4}=1: 1+y_{4} z_{4}+x_{3}^{3} y_{4}^{2} z_{4}^{3}=0$. Sing if also $3 x_{3}^{2} y_{4}^{2} z_{4}^{3}=0, y_{4}+3 x_{3}^{3} y_{4}^{2} z_{4}^{2}=0$, $z_{4}+2 x_{3}^{3} y_{4} z_{4}^{3}=0$ No solutions, so nonsingular.
- $y_{4}=1: \quad x_{4}^{2} y_{1}+z_{4}+y_{1}^{4} z_{4}^{3}=0, \quad 2 x_{4} y_{1}=0, x_{4}^{2}+4 y_{1}^{3} z_{4}^{3}=0,1+3 y_{1}^{4} z_{4}^{2}=0$. No solutions.
- $z_{4}=1$ : Similar to above case: no solutions.

So result of blowing up is NONSINGULAR. For later use, not that this applies to anything of the form $x^{2}+y z+y z($ polynomial in $y$ and $z)$.

Now look at the other singularity, $x_{3}^{2}+y_{3}^{2} z_{2}+y_{3} z_{2}^{2}=0$ at $\left(x_{3}: y_{3}: z_{3}\right)=$ ( $0: 0: 1$ ). Blowup introducing ( $x_{5}: y_{5}: z_{5}$ ).

- $x_{5}=1: 1+x_{3} y_{5}^{2} z_{5}+x_{3} y_{5} z_{5}^{2}=0$ Nonsingular
- $y_{5}=1: \quad x_{5}^{2}+y_{3} z_{5}+y_{3} z_{5}^{2}=0$ Singular if also $2 x_{5}=0, z_{5}+z_{5}^{2}=0$, $y_{3}+2 y_{3} z_{5}=0$. Two singularities, at $x_{5}=0, y_{3}=0, z_{5}=0$ or -1 .
- $z_{5}=1$ : Similar to previous case: Two singularities, at $x_{5}=0, z_{2}=0$, $y_{5}=0$ or -1 .

So there are THREE singularities at $\left(x_{5}: y_{5}: z_{5}\right)=(0: 0: 1)$ or $(0: 1$ : $0) \operatorname{or}(0: 1:-1)$. Fortunately each of these 3 singularities looks like $x^{2}+y z+$ $y z$ (monomial in $y, z$ ) so can be resolved with 1 further blowup.

Summary: altogether we needed 8 blowups, using a total of 27 variables, as each blowup introduced 3 new variables. Problem with repeated blowups: notation becomes a mess. Some authors reuse $x, y, z$ each time, though this becomes confusing. In general things can be a lot more complicated: for example, there may be singular sets of $\operatorname{dim}>0$ which require blowing up along more complicated varieties (see below), and even if there are non to start with, blowing up a singular point may produced a singular set of $\operatorname{dim}>0$.

Remark: the intersection of $v^{2}+w^{2}+x^{2}+y^{3}+z^{5+6 k}=0$ with a small sphere around the origin in $C^{5}$ is one of Milnor's manifolds homeomorphic but not diffeomorphic to $S^{7}$.

Example $52 x^{4}+y^{4}=z^{2}$. Used by Fermat to solve Fermat's last theorem for exponent 4. Only singularity is at origin: dimension 0. Blow it up using $\left(x_{1}: y_{1}: z_{1}\right)$ as coordinates for projective space. Nonsingular along $z_{1}=1$. But along $y_{1}=1$ we get $x_{1}^{4} y^{2}+y^{2}=z_{1}^{2}$ which is singular along the LINE $z_{1}=0$, $y=0$. So blowing up has increased the dimension of the singular set. (Blowing up along this line resolves the singularity.)

Example 53 Blowups with a poor choice of center can even make a singularity worse. $x^{2}-y z=0$ blown up along line $y=z=0$ gives $x^{2}-y^{2} z=0$. Here the center of the blowup sticks out from the variety. Can even increase the multiplicity of a singularity such as $w^{2} x^{2}=y^{2} z^{2}$.

Example 54 Why do people care about resolution of singularities? Many results use it for proofs. Example: analytic continuation of power $|f|^{s}$ of a polynomial $f$. (Special case: analytic continuation of $\Gamma$.) Idea (Atiyah): resolve singularity of polynomial so that inverse image has only normal crossing singularities, so in local coordinates polynomial looks like $x_{1}^{n_{1}} x_{2}^{n_{2}} \ldots$ which is easy to do as we can continue $x^{s}$ using $\frac{d}{d x} x^{s}=s x^{s-1}$ (as in proof for $\Gamma$ ). Since the map from the resolution is proper, we can push forward distributions, as the pullback of a compactly supported function is still compactly supported.

Hironaka's theorem is not really necessary: Bernstein found a more elementary proof using Bernstein polynomials that avoids it. Idea is to find a differentiable operator $D$ and a (Bernstein) polynomial $b$ such that $D f\left(x_{1}, \ldots\right)^{s}=$ $b(s) f\left(x_{1}, \ldots\right)^{s-1}$.

The Malgrange Ehrenpreis theorem is an immediate consequence: By taking Fourier transforms, finding a fundamental solution of a constant coefficient differentiable operator is equivalent to finding a distributional inverse of a polynomial $f$. But this is given by the constant term of the meromorphic distributionvalued function $f^{s}$ of $s$ at $s=-1$.

Example 55 Number fields. $\boldsymbol{Z}[\sqrt{-3}]$ is singular at prime 2. Look at local ring $Z_{2}[\sqrt{3}]$. Max ideal $\mathfrak{m}$ generated by $2, \sqrt{-3}-1$. Square $\mathfrak{m}^{2}$ generated by $4,2 \sqrt{3}-2$. Maps onto $\boldsymbol{Z} / 4 \boldsymbol{Z}[\sqrt{3}] /(2 \sqrt{3}-2)$ of order 8 . So $\mathfrak{m} / \mathfrak{m}^{2}$ has order 4 and tangent space has dimension 2. Integral closure is $\boldsymbol{Z}[(\sqrt{-3}+1) / 2]$. This times $\mathfrak{m} / \mathfrak{m}^{2}$ has order 2 .

### 1.5.3 Completions

Examples: Completion $k[x]$ is $k[[x]]$, completion of local ring $Z_{(p)}$ is $Z_{p}$.
Completion $\hat{R}$ of local ring $R$ is inverse limit of $R / \mathfrak{m}^{n}=$ completion in Krull topology.

Map from $R$ to $\hat{R}$ injective ( $\cap \mathfrak{m}^{n}=0$, Krull topology Hausdorff) if $R$ Noetherian but not in general even for natural examples: example local ring of germs of SMOOTH functions near 0 , or even worse $\bigcup k\left[\left[x^{1 / n}\right]\right]$, where $\mathfrak{m}=\mathfrak{m}^{2}$.

Key property is Hensel's lemma, stating that solutions in $k$ can often be lifted to solutions in $\hat{R}$, by lifting to $R / \mathfrak{m}, R / \mathfrak{m}^{2}, R / \mathfrak{m}^{3}, \ldots$. Many variations. Typical example: If $f_{0}(Z)=g_{0}(Z) h_{0}(Z)$ and $g_{0}, h_{0} \in k[Z]$ are COPRIME then this lifts to a factorization $f=g h$ in $\hat{R}[\mathrm{Z}]$. Proof: suppose we have a factorization mod $\mathfrak{m}^{n}$. Want to lift this to a factorization mod $\mathfrak{m}^{n+1}$. Need to find $a, b \in \mathfrak{m}^{n} / \mathfrak{m}^{n+1}$ with $g_{0} a+h_{0} b=$ something, which has a solution as $g_{0}, h_{0}$ are coprime.

Application: $y^{2}=x^{3}+x^{2}$. Take $R$ to be local ring at 0 . Then $Z^{2}=x+1$ has roots $Z= \pm 1$ in $k$, which lift to solutions in $\hat{R}$ if char $\neq 2$, so $y^{2}-x^{2}(x+1)$ factorizes as $(y-x+\ldots)(y+x+\ldots)$. Note that this FAILS in char $2 ; g_{0}, h_{0}$ are no longer coprime. So curve looks analytically like xy $=0$ except in char 2 where it has a cusp.

Nasty properties of completions: completion of an integral local ring need not be integral (see above); completion of a reduced local ring need not be reduced. Henselization much better.

### 1.5.4 Elimination theory

Abhyankar' slogan: "Eliminate the eliminators of elimination theory"
Briefly mentioned in theorem 5.7A, but very important. Problem: eliminate $y$ from $x^{3} y^{4}-7 x^{2}+y^{6}-x y^{8}$ and $3 x^{2} y^{5}+4 y^{2}+7 x^{6}+x^{4} y^{7}$. Intersection of 2 plane curves. Some degree 99 polynomial in $x$. We want to find an EXPLICIT FORMULA for it!

General problem: Given polynomials $f(x)=a_{m} x^{m}+\ldots$ and $g(x)=b_{n} x^{n}+$ ..., what is condition for them to have a common root? If they do then $f(x) p(x)=g(x) q(x)$ where $\operatorname{deg}(p)<n, \operatorname{deg}(q)<m$ for some $p, q$ as we can take
$p=g /(x-\alpha), q=f /(x-\alpha)$. This is a set of linear equations so condition for a nontrivial solution is

$$
\left|\begin{array}{ccccc}
a_{m} & a_{m-1} & a_{m-2} & \ldots & \\
0 & a_{m} & a_{m-1} & & \\
& & & a_{0} & 0 \\
0 & & & a_{1} & a_{0} \\
b_{n} & b_{n-1} & & 0 & 0 \\
0 & b_{n} & & b_{0} & 0 \\
0 & & & b_{1} & b_{0}
\end{array}\right|=0 n \text { rows for } a^{\prime} s, m \text { rows for } b^{\prime} s
$$

(Determinant of Sylvester matrix) Also equal to const $\times \Pi(\alpha-\beta)$.
More precisely, this condition is equivalent to $f$ and $g$ either have a common root or both have zero leading coefficients ("common root at infinity"). Another way of putting this is that HOMOGENEOUS polynomials have a common nontrivial solution. This determinant is called the RESULTANT of $f$ and $g$. (Compare Bezoutiant, catalecticant, determinant, harmonizant, canonizant,...)

Example: What is condition for $f$ to have a multiple zero (or leading coefficient 0 )? A. $f$ and $f^{\prime}$ have common root, so resultant of $f$ and $f^{\prime}$ is zero. Example for cubic $x^{3}+\mathrm{bx}+c$

$$
\left|\begin{array}{lllll}
1 & 0 & b & c & 0 \\
0 & 1 & 0 & b & c \\
3 & 0 & b & 0 & 0 \\
0 & 3 & 0 & b & 0 \\
0 & 0 & 3 & 0 & b
\end{array}\right|=4 b^{3}+27 c^{2}
$$

Geometric meaning: Consider $f$ and $g$ to be homogeneous polynomials with coefficients in $k\left[y_{1}, \ldots, y_{k}\right]$ Then $f$ and $g$ define hypersurfaces $H_{f}, H_{g}$ in $A^{k} \times P^{1}$. Resultant gives projection of $H_{f} \cap H_{g}$ in $A^{k}$. In particular IMAGE OF CLOSED SET $H_{f} \cap H_{g}$ IS CLOSED!

More generally we want to show that $Y \times Z \rightarrow Y$ is closed for any projective variety $Z$. (Analogue for $A^{k} \times A^{1} \rightarrow A^{1}$ is false ( $x y=1$ projected on $x$ does not have closed image. Over reals it is not even true that a polynomial maps from $\boldsymbol{R}^{n} \rightarrow \boldsymbol{R}$ has closed image: for example $x^{2}+(x y-1)^{2}$.) This is the analogue of compactness for projective varieties. (Usual definition of compactness useless, as all affine varieties are compact.) Recall concept of proper maps for topological spaces: $X \rightarrow Y$ is called proper if it is continuous and universally closed. Equivalent to continuous+closed+fibers compact. For locally compact Hausdorff spaces this is equivalent to continuous + inverse image of compact is compact. For Hausdorff spaces, compact is equivalent to (projection to a point is proper). So we define a map of varieties to be proper if it is universally closed (for Zariski topology on products!)

Now check that $P^{1} \rightarrow$ point is proper (analogue of saying $P^{1}$ is compact in complex topology). Sufficient to show $P^{1} \times A^{k} \rightarrow A^{k}$ is closed. Suppose that a closed set $S$ in $P^{1} \times A^{k}$ is given by the zeros of $f_{1}, f_{2}, \ldots$, where
each is a polynomial in $X, Y, Z_{1}, \ldots, Z_{k}$, homogeneous in $X, Y$. Look at resultant of $t_{1} f_{1}\left(X, Y, Z_{1}, \ldots\right)+t_{2} f_{2}\left(X, Y, Z_{1}, \ldots\right)+\ldots$ and $s_{1} f_{1}\left(X, Y, Z_{1}, \ldots\right)+$ $s_{2} f_{2}\left(X, Y, Z_{1}, \ldots\right)+\ldots$ considered as homogeneous polynomials in $X$ and $Y$. This is a polynomial in $s_{1}, s_{2}, \ldots t_{1}, t_{2}, \ldots Z_{1}, \ldots, Z_{k}$. Then the projection of $S$ is given by the vanishing of all coefficients of $s^{\alpha} t^{\beta}$. So the image of $S$ is closed.

Now we want to show that $P^{n} \rightarrow$ point is proper. This would be trivial by induction on $n$ if $P^{n}=P^{n-1} \times P^{1}$, but this is not true. It is close to being true: correct version is: blowup of $P^{n}$ at a point is a (nontrivial) $P^{1}$-bundle over $P^{n-1}$. To see this look at graph $Z$ of correspondence from $P^{n} \rightarrow P^{n-1}$. $Z$ is the set of pairs $\left(\left(x_{0}: \ldots: x_{n}\right),\left(y_{1}: \ldots: y_{n}\right)\right)$ with $x_{i} y_{j}=x_{j} y_{i}$. The $\operatorname{map} Z \rightarrow P^{n}$ is an isomorphism except that it maps a whole $P^{n-1}$ to ( $0: . .: 0: 1$ ) so is blowup of $P^{n}$ at this point. Moreover $Z \rightarrow P^{n-1}$ is locally a projection: over the hyperplane $y_{i}=1$ we have $x_{j}=x_{i} y_{j}$ so if we map $\left(\left(x_{0}: \ldots: x_{n}\right)\right.$ to $\left(x_{0}: x_{i}\right) \times\left(x_{1}, \ldots, x_{i-1}, x_{i+1}, \ldots\right)$ we see that over the hyperplane we get a projection from $P^{1} \times A^{n-1} \rightarrow A^{n-1}$.

Since the map from $Z \rightarrow P^{n-1}$ looks locally like $P^{1} \times A^{n-1} \rightarrow A^{n-1}$ it is proper. So the map from $P^{n}$ to a point is proper by induction.

Note use of blowup to change a rational map into a regular map defined everywhere: common technique.

Remark: For $n=2$ the surface $Z$ is an example of a ruled surface over $P^{1}$, not isomorphic to either $P^{2}$ or $P^{1} \times P^{1}$. (Hirzebruch surface.)

Alternative short proof using Determinantal varieties. Suppose $f_{1}, f_{2}, \ldots$ are homogeneous polynomials in $Z_{1}, \ldots$ We want to show that the condition that they have a common zero is closed in their coefficients. But they have no common zero if and only if their ideal contains $\left(Z_{1}, \ldots\right)^{d}$ for some $d$ by the Nullstellensatz. For each fixed $d$ the condition that linear combinations of the $f$ contain all degree $d$ monomials in the $Z$ 's just says that a certain linear map with coefficients that are polynomials in the coefficients of the $f$ 's is onto. But by the theory of determinantal varieties being onto is a (horrendously complicated) open condition on the linear map. So the points where the $f$ have no common zero is a union over $d$ of open subsets, so is open. (Nonconstructive as we take a union over $d$; can be made constructive by estimating max necessary $d$.)

These proofs suggest that although the image of a closed set is closed, it can be VERY complicated to describe explicitly as the dimension grows: the proofs require more than exponentially large numbers of equations with more than exponentially large numbers of nonzero coefficients.

Example 56 Newton's theorem that smooth ovals cannot be algebraically integrated. Used by Newton to show that the position of a planet in a periodic orbit for a smoothly varying central force cannot be given by an algebraic function of time (though its orbit can often be described algebraically of course). Since area swept out is proportional to time, this reduces to the question: given a smooth oval, show that the area cut off by a secant is not an algebraic function of the secant. (For non-smooth ovals there are lots of counterexamples: triangles, $y^{2}=x^{2}-x^{4}$. This caused a lot of confusion since Newton did not explicitly state the condition that the oval most be smooth, which was finally
pointed out by Arnold.) Newton's proof: consider the spiral given by (distance from center)=area swept out. Suppose this is locally algebraic. Since it is also smooth, there are no singular points so it is algebraic. But then it has an infinite number of intersection points with a line through the origin, which contradicts "Bezout's theorem" (stated by Newton.) In the case of triangles etc, Newton's spiral is a union of a countable number of algebraic curves spliced together.

### 1.6 Nonsingular curves

Basic invariant (of complex curves) is the genus. Some examples:
Genus 0: Projective line.
Genus 1: Elliptic curves. Take $\boldsymbol{C} /$ lattice $\{1, \tau\}$ and use $\wp^{\prime 2}=4 \wp^{3}+b \wp+c$ to map it to a cubic curve $y^{2}=4 x^{3}+b x+c$. This gives it as branched double cover of plane with 4 branch points (don't forget possible branch point at infinity). Any elliptic curve can be put into the form $y^{2}=x(x-1)(x-\lambda)$ and 2 are the same if and only if there is an aut of $P^{1}$ taking the set $\left\{0,1, \infty, \lambda_{1}\right\} \rightarrow\left\{0,1, \infty, \lambda_{2}\right\}$. This is possible if $\lambda_{2}$ is $\lambda_{1}, 1-\lambda_{1}, 1 / \lambda_{1}, 1-1 / \lambda_{1}, \lambda_{1} /\left(\lambda_{1}-1\right), 1 /\left(1-\lambda_{1}\right)$, image of $\lambda_{1}$ under a group of order 6 given by permutations of $\{0,1, \infty\}$. So moduli space is affine line modulo this group of order 6 . Need rational function of $\lambda$ invariant under this group: use elliptic modular function $j=256\left(\lambda^{2}-\lambda+1\right) / \lambda^{2}(\lambda-1)^{2}$. This is the $j$-invariant of an elliptic curve: 2 complex elliptic curves are isomorphic if and only if they have the same $j$-invariant. So (course) moduli space $=$ affine line. (This is misleading: elliptic curves $y^{2}=x^{3}-x, y^{2}=x^{3}-1$ with aut groups that are larger than normal really correspond to $1 / 2$ or $1 / 3$ of a point in the moduli space, and this cannot be described in a completely satisfactory way with varieties or even schemes. The definitive description uses the moduli STACK of elliptic curves, which can handle automorphisms in a satisfactory way. Similarly almost any nontrivial moduli problem involves stacks.) Description of $j$ in terms of $\tau$ is quite complicated: $j=q^{-1}+744+196884 q+\ldots$ where $q=e^{2 \pi i \tau}$; see any good book on modular forms for details. Weird fact: coefficients of $j-744$ are the dimensions of the pieces of the natural graded representation of the monster simple group: e.g. $196884=1+196883$ (McKay).

Genus 2: Hyperelliptic curves: a double cover or projective line with $2 n$ branch points has Euler characteristic is $2 \times 2-2 n$ so genus is $n-1$, so for 6 branch points we get genus 2. Moduli space is given by sets of 6 distinct points on $P^{1}$ modulo action of $\mathrm{PSL}_{2}(C)$. This is essentially the same as the problem of finding invariants of a sextic binary form, which is quite hard. (Answer: moduli space looks like $A^{3}$ modulo action of a cyclic group of order 5 taking $(x, y, z) \rightarrow\left(\zeta x, \zeta^{2} y, \zeta^{3} z\right)$ where $\zeta^{5}=1$. Ring of invariants contains by $x^{5}, x^{3} y, x y^{2}, y^{5}, x^{2} z, x z^{3}, z^{5}, y z$.) No such description of moduli space seems to be known for higher genus.

Genus 3: Some are hyperelliptic, but many are not. Example: degree 4 nonsingular curve in plane. Work out genus of degree $d$ nonsingular curve by considering it as a $d$-fold cover of a projective line: in general it will have $d(d-1)$ branch points of order 2 , so Euler characteristic is $2 d-d(d-1)=2-2 g$, so $g=(d-1)(d-2) / 2$. We get a 6 -dimensional family of such curves (space of
polynomials is dimension 15 , subtract 1 as we want projective space, subtract another 8 for automorphisms of projective plane.) Hyperelliptic curves of genus 3 form a family of dimension $8-3=5$. Example (Trott): $144\left(x^{4}+y^{4}\right)-$ $225\left(x^{2}+y^{2}\right)+350 x^{2} y^{2}+81=0$. Graph is 4 beans, so has 28 real bitangents. In general nonsingular degree 4 curves have 28 bitangents touching at 56 special points. (These are not Weierstrass points: more functions than expected with poles just at this point).

Genus 4: Cannot be obtained as nonsingular plane curves. Given by intersection of cubic and quadric in $P^{3}$. Genus 5 given by intersection of 3 quadrics in $P^{4}$. Representing curves of higher genus gets hard: can use embeddings into projective space (e.g. canonical embedding), or embeddings into plane with singularities, or branched coverings of the plane, or quotients of upper half plane by discrete groups

General genus: Pick lots of points $x, x_{1}, \ldots x_{n}$ in projective line. Choose $n$ transpositions on $d$ points with product 1 , acting transitively on the $d$ points. Construct Riemann surface by choosing cuts from $x$ to $x_{n}$ then joining $d$ copies of the cut projective line these up using the transpositions. Result has Euler characteristic $2 d-n$.

Hurwitz curves: what is most symmetrical complex algebraic curve of given genus? Genus 1 has infinite automorphism group, so look at genus ¿1. Hurwitz bound: automorphism group has order at most $84(g-1)$. Idea of proof: look at orbifold quotient. This has orbifold Euler characteristic $(2 g-2) /|G|<0$. On the other hand, if the underlying (orientable) surface has genus $h$ and conical singularities of orders $p_{1}, p_{2}, \ldots$ then the orbifold Euler characteristic is

$$
2-2 h-\left(1-1 / p_{1}\right)-\left(1-1 / p_{2}\right)-\ldots
$$

The maximum negative value of this is $-1 / 42$ with $h=0, p_{1}=2, p_{2}=3, p_{3}=7$. To see this look at various cases. First, $h$ must be 0 or the value is at most $-1 / 2$. Second, if there are at most 2 conical points the Euler characteristic is positive. Third, if there at at least 4 conical points and the Euler characteristic is negative it must be at most $-1 / 6$ coming from conical points of orders $2,2,2$, 3. So there are exactly 3 conical points. Fourth, if no conical point has order 2 then the possibilities are $3,3,3$ or $3,3,4$, and so on, so the Euler characteristic is at most $-1 / 12$. So we can assume one conical point has order 2 . If there are 2 conical points of order 3 then the Euler characteristic is positive, so the other two conical points have orders at least 3. If neither has order 3 , the smallest possibilitities are $2,4,4$ and $2,4,5$ with Euler characteristics $0,1 / 20$. So we can assume one point has order 2 and another has order 3 and the third has order at lest 3 . If the third has order $3,4,5,6,7,8 \ldots$ the Euler characteristic is $1 / 6,1 / 12,1 / 30,0,-1 / 42,-1 / 24, \ldots$ So we get the Hurwitz bound as the largest possible negative value of the Euler charcateristic is $-1 / 42$. In fact we get more, since the second largest possible value is $-1 / 24$, so if a finite group of automorphisms does not achieve the Hurwitz bound then it has order at most $48(g-1)$.

So $(2 g-2) /|G| \leqslant-1 / 42$ or $|G| \leqslant 84(g-1)$. Moreover in this case $G$ must be a quotient of the orbifold fundamental group of the orbifold above, so is
generated by elements of orders $2,3,7$, and product 1 . Conversely any such finite group is the automorphism group of a Hurwitz surface.

Exercise: classify the 17 wallpaper groups by finding all orbifolds of Euler characteristic 0 . These can also have folds and angles as singularities, and the underlying topological surface can be a sphere or disc or torus but also be a non-orientable surface such as a Klein bottle, Moebius band, projective plane.

Example 57 There is no Hurwitz surface of genus 2. In this case the automorphism group $G$ has order 84 . But by Sylow, any group of order 84 has a normal subgroup of order 7 , and the quotient group of order 12 has a normal subgroup of order 4 or 3 . In the first case every element of order 2 or 7 is in the normal subgroup of order 28 , which has no elements of order 3 . Similarly in the second case every element of order 3 or 7 is in the normal subgroup of order 21 , which has no elements of order 2. So there is no Hurwitz group of order 84.

So the maximum possible order of the automorphism group of a genus 2 surface is $48(g-1)=48$. There is in fact a surface with this order of automorphism group, given by taking the double branched cover of the projective line branched at $0,1,-1, i,-i, \infty$ (the corners of an octahedron). The subgroup of $P S L_{2}(C)$ fixing this set of 6 points has order 24, generated by $z \rightarrow i z$ and $z \rightarrow(1+z) /(1-z)$, and is isomorphic to the symmetric group $S_{4}$ on 4 points. The group of order 48 is a central extension of this where the center exchanges the two branches. (This is a non-split extension: for example elements of order 4 in $S_{4}$ lift to elements of order 8 in the automorphism group. It has a presentation $x^{2}=y^{3}=z^{8}=x y z=1, z^{4}$ in the center.) The hyperelliptic curve cannot be embedded as a non-singular plane curve, but can be constructed as an abstract variety by taking two copies of $y^{2}=x\left(x^{2}+1\right)\left(x^{2}-1\right)$, and gluing the open subsets $x \neq 0$ using the involution $x \rightarrow 1 / x, y \rightarrow y / x^{3}$.

Example 58 There were 5 cases where the Euler characteristic is 0 given by orbifold points of orders (), $(2,2,2,2),(3,3,3),(2,4,4),(2,3,6)$, . These correspond to the 5 possible cyclic groups acting on elliptic curves, of orders $1,2,3$, 4, 6 .

Example 59 The cases where the Euler characteristic is positive correspond to finite groups acting on a sphere together with some "bad" orbifolds not corresponding to any manifold.

Example 60 Suggested by Francesco Polizzi on mathoverflow. A Hurwitz curve of genus 3 is the Klein quartic: $x^{3} y+y^{3} z+z^{3} x=0$. This is nonsingular (check) so has genus $(d-1)(d-2) / 2=3$. It is the only genus 3 Hurwitz curve with automorphism group of order Hurwitz's upper bound $84(g-1)=168$; automorphism group is simple group $\mathrm{PSL}_{2}\left(\boldsymbol{F}_{7}\right)=\mathrm{SL}_{3}\left(\boldsymbol{F}_{2}\right)$. Obvious automorphisms $x \rightarrow y \rightarrow z \rightarrow x$ and $x \rightarrow \zeta^{4} x, y \rightarrow \zeta^{2} y, z \rightarrow \zeta z$ with $\zeta^{7}=1$ generate a subgroup of order 21.

Proof that it has automorphism group of order 168: The group $\mathrm{PSL}_{2}(Z)$ has elements $S=\left(\begin{array}{cc}0 & 1 \\ -1 & 0\end{array}\right), T=\left(\begin{array}{ll}1 & 1 \\ 0 & 1\end{array}\right)$ with $S^{2}=(\mathrm{ST})^{3}=1$ and in
$\mathrm{PSL}_{2}\left(\boldsymbol{F}_{7}\right)$ the image of $T$ has order 7 , so we get a Hurwitz group or order 168. It has a subgroup of order 21 acting on 3 -dim space as above. The Klein quartic is the only quartic invariant under this subgroup. It is not that easy to write down an explicit automorphism not in this subgroup.

Following are essentially equivalent:

- Nonsingular projective curves, up to isomorphism of curves
- Curves, up to birational isomorphism
- Finitely generated algebraic function fields over $k$ of transcendence degree 1, up to isomorphism
- (Over C) Compact connected Riemann surfaces.

Nonsingular curves $\rightarrow$ curves $\rightarrow$ function fields easy, as is nonsingular curves $\rightarrow$ Riemann surfaces.

Compact Riemann surfaces $\rightarrow$ algebraic function fields: take field of meromorphic functions. Hard problem: show that enough meromorphic functions exist. Not easy to show there are any nonconstant ones. Example: $(\boldsymbol{C}-0) /(z=$ $2 z)$ : find a meromorphic function $f$ on $\boldsymbol{C}-0$ with $f(z)=f(2 z)$. Same problem in higher dimensions has no solution: Hopf surface $=\left(\boldsymbol{C}^{2}-0\right) /\left(\left(z_{1}, z_{2}\right)=\right.$ $\left.\left(2 z_{1}, 2 z_{2}\right)\right)$ is a compact 2-dimensional complex manifold that is NOT projective!

Function fields $\rightarrow$ Curve: By field theory, the function field has a separating transcendence base, which has just one element $x$. It is a finite separable extension of $k(x)$ so is a simple extension of the form $k[x, y]$ which as $y$ is algebraic over $x$ are related by some nonzero polynomial $f(x, y)=0$. This gives the equation of some curve.

Curve $\rightarrow$ nonsingular projective curve. Making the curve projective is trivial, so the problem is to show that we can resolve the singularities of a curve. More than 20 ways to do this. Original method due to Newton using Newton polygons, Puiseux expansions as follows

### 1.6.1 Newton's method

Think of $f(x, y)$ as a polynomial in $y$. Allow rational powers of $x$. Then roots can be written as Puiseux series = Taylor series in $x^{1 / N}$ for some integer $N$. (Puiseux series and Taylor series both invented by Newton.) Example: $y^{2}=x^{3}+x^{4}$. Look at Newton polygon of $f$, and find leading edge containing some $y^{N}$ using method of rotating ruler. Terms on this leading edge have lowest weighted degree, so form homogeneous polynomial in $x$ and $y$ for suitable weights of $x, y$. Idea is that we substitute to reduce $N$ or keep $N$ same and reduce slope of leading edge. 2 cases:

- If not all roots equal, then substitute $y \rightarrow y-a x^{r / s}$ to reduce least power of $y$ in $f$. This case only occurs a finite number of times as $N$ is finite and a positive integer.
- All roots equal. Substitute $y \rightarrow y-a x^{r / s}$ to reduce slope of leading edge. Can occur an infinite number of times, but this converges to a Puiseux series for $y$.

A slight extension of this shows that the field of Puiseux-Laurent series over $\boldsymbol{C}$ is algebraically closed. Proof similar to proof that if $f(x, y)=0$ then $y$ is a Puiseux series, but allow $f$ to be Puiseux series in $x$ rather than just a polynomial. A rare example of an explicit algebraically closed field. Field of Laurent series over $\boldsymbol{C}$ has a unique extension of each degree, like finite fields. Such fields are sometimes called quasi-finite fields. (Check definition, relation to theory of finite fields.)

What does this have to do with resolution of singularities? Idea: curve looks analytically locally like a product of curves $y=a x^{r / s}+\ldots$ or $y^{s}=$ $b x^{r}+$ higher powers of $x$. (Note that different analytic branches can be the same algebraic branch: example $y^{2}=x^{3}+x^{2}$.) Blowing up reduces $r$ or $s$ until one of them is 1 , in which case curve is nonsingular. (When blowing up a point on an arbitrary curve it can be hard to see that the point has been simplified.)

This is not quite a complete proof of resolution as we have only shown how to resolve each analytic branch. So we will introduce 2 invariants to measure nastiness of a singularity and show that blowing up improves invariants until curve is nonsingular. Invariants are:

1. The multiplicity of the singularity
2. The min value of the slope of the leading edge of the Newton polygon, taken over ALL choices of local analytic coordinates with $y^{N}$ a min degree term and NO terms $y^{N-1} x^{*}$ (change coordinates by ( $x, y+$ power series in $x$ ); this needs char $=0$ ). This slope is $\leqslant 1$.

Look at effect of blowing up on these invariants. This depends on the roots of the polynomial of terms of lowest weighted degree, on the leading edge of the Newton polygon.

1. If this polynomial has more than 1 root, then blowing up reduces the multiplicity of the singularity, essentially because it will separate the roots. This can only happen a finite number of times.
2. If this polynomial has all roots the same, then slope of leading edge is less than 1 as coefficient of $y^{N-1} x$ is 0 . Then blowing up will increase the slope of the leading edge. If this new slope is greater than 1 then the multiplicity is reduced.

Note that we need to eliminate terms $y^{N-1} x$ otherwise we seem to end up going in circles.

### 1.6.2 Other methods

Riemann's method: construct Riemann surface of a complex algebraic curve or function field. Hartshorne gives an algebraic version of this.

One word method: normalization. Normalization of an integral domain=integral closure in quotient field: normal ring. A Noetherian ring is normal if and only if it is nonsingular in codimension $1\left(A_{p}\right.$ regular whenever $p$ has height at most 1 ) and if $p$ has height at least 2 then $A_{p}$ has depth at least 2 (Serre), so this resolves singularities of curves. No analogue known in higher codimension, and normalization not really useful for resolution in dim at least 3. (In dim 2 a common method is to alternate normalization with blowing up singular points, but this does not generalize.) Used in number theory: ring of integers is integral closure of $\boldsymbol{Z}$ in number field.

### 1.7 Intersections in projective space

### 1.7.1 Hilbert polynomials

Problem: Suppose we have a finitely generated graded module $M=\oplus M_{n}$ over a finitely generated graded algebra $R$ over a field. How does $\operatorname{dim}\left(M_{n}\right)$ grow? Encode as power series $f_{M}(x)=\sum x^{n} \operatorname{dim}\left(M_{n}\right)$. Then this function is RATIONAL. Proof by induction on number of generators of $R$. Suppose $r$ is in a finite set of generators and has degree $n$. Look at

$$
0 \rightarrow \operatorname{ker}(r) \rightarrow M \rightarrow M(n) \rightarrow M(n) / r M(n) \rightarrow 0
$$

where $M(n)$ is $M$ with grading shifted by $n$. This gives

$$
f_{\operatorname{ker}(r)}-f_{M}+f_{M(n)}-f_{M(n) / r M(n)}=0
$$

But by induction the first and last terms are rational functions, and $f_{M(n)}=$ $x^{n} f_{M}$, so $f_{M}$ is rational. This also shows the denominator can be taken as $\Pi\left(1-x^{n_{i}}\right)$ where the $n_{i}$ are the degrees of the generators.

Important special case: if all generators have degree 1 then denominator is $(1-x)^{n}$ whose coefficients are polynomials in $m$ for large $m$, so for SUFFICIENTLY LARGE $m, \operatorname{dim}\left(M_{m}\right)$ is a POLYNOMIAL in $m$ called the Hilbert polynomial.

Polynomials that are integer-valued on the integers need not have integral coefficients: $x(x-1) / 2$. Spanned by $1, x, x(x-1) / 2, x(x-1)(x-2) / 3!, \ldots$, $\binom{x}{n}=x(x-1) \ldots(x-n+1) / n!$ ! $\ldots$ (Proof: $\binom{x}{n}$ is 0 for $x=0, \ldots n-1$ and 1 for $x=n$., etc.) So leading coefficient is $d x^{n} / n$ ! for some integer $d$. Most important invariants are $n$ and $d$; lower coefficients tend to vary with choice of grading of $M$ so not so useful.

Useful variations: replace dimension of vector space over a field by any other invariant that is additive on exact sequences, such as length of a module.

### 1.7.2 Dimension of local rings

If $R$ is a Noetherian local ring then $\oplus \mathfrak{m}^{n} / \mathfrak{m}^{n+1}$ is a graded ring, finitely generated over the field $R / \mathfrak{m}$ by degree 1 elements, so has Hilbert function.

For a Noetherian local ring the following are equal:

1. geometric dimension $=\max$ length of chain of prime ideals -1
2. $1+$ deg of Hilbert polynomial of $\oplus \mathfrak{m}^{n} / \mathfrak{m}^{n+1}$
3. Smallest number of elements of $\mathfrak{m}$ not contained in any other prime ideal.
4. Smallest system of parameters (set of elements of $\mathfrak{m}$ generating a cofinite ideal).

Proofs are hard commutative algebra.
Problem: most of these almost impossible to calculate directly. But Hilbert polynomial is easy to calculate.

### 1.7.3 Degree of a projective variety

If $I \subseteq R=k\left[x_{0}, \ldots, x_{n}\right]$ is the graded ideal of a projective variety then $R / I$ is a graded module over $R$ so has Hilbert polynomial. Then degree $r$ of Hilbert polynomial $=$ dimension of variety, and degree of variety is defined to be $r!\times$ leading coef.

Example 61 Projective space $P^{n}$. dimensions are $1, n+1,(n+1)(n+2) / 2!, \ldots,(n+$ 1) $\ldots(n+k) / k!=\binom{n+k}{n}=k^{n} / n!+\ldots$ so dimension is $n$ and degree is 1 .

Example 62 Hypersurface of degree $d$ in $P^{n}$. Hilbert polynomial is $\binom{n+k}{n}$ -$\binom{n+k-d}{n}=d k^{n-1} /(n-1)$ ! so dimension is $n-1$ and degree is $d$.

Example 63 Twisted cubic: $\mathrm{wz}=\mathrm{xy}, x^{2}=\mathrm{wy}, y^{2}=\mathrm{xz}$. Basis of coordinate ring: 1; w, x, y, z;

In general cant have $x^{2}, y^{2}, \mathrm{xy}$, so get $w^{i} z^{k-i}, w^{i} x z^{k-i-1}, w^{i} y z^{k-i-1}$ which is $k+1+k+k=3 k+1$. So $\operatorname{dim}=1$ and degree $=3$.

For a projective variety the Euler characteristic $\chi$ is defined to be constant term of Hilbert polynomial (coherent cohomology Euler characteristic of sheaf of regular functions, so does not depend on embedding of variety into projective space). For historical reasons $(-1)^{\operatorname{dim}}(\chi-1)$ is called the arithmetic genus.

Example 64 Arithmetic genus of a plane curve of degree $d$. Hilbert polynomial is $\binom{2+k}{2}-\binom{2+k-d}{2}=1-(2-d)(1-d) / 2$ so arithmetic genus is $(d-1)(d-2) / 2$. For nonsingular complex curves this is topological genus.

Remark. Hilbert polynomial is Euler characteristic of $\mathcal{O}(n)$, and higher cohomology groups all vanish for $n$ large.

Remark 2 The Hilbert polynomial of a closed subvariety or subscheme is essentially the only discrete invariant. Hartshorne showed that 2 points in Hilbert scheme are in same connected component if and only if they have the same Hilbert polynomial. However connected components of Hilbert scheme often have many irreducible components (with horrendous singularities).

### 1.7.4 Hironaka's example

Hironaka gave example of a 3-dim nonsingular abstract variety that is not projective. Take 2 curves in a nonsingular 3 -fold intersecting transversely at 2 points $P, Q$. On $X-P$ blowup first one curve then the strict transform of the other. On $X-Q$ do in other order. Then glue together. TODO

### 1.7.5 Bezout's theorem

Old style: Intersection of 2 GENERIC curves of degrees $m, n$ in $P^{2}$ has $m n$ points. More generally, intersection of hypersurfaces of degrees $n_{1}, \ldots$ has $n_{1} \times \ldots$ points. Old style "proof": vary coefficients of each hypersurface so it degenerates into a union of hyperplanes, and hope that the number of intersection points does not change under this process.
"Generic" means: theorem often true, but there sure seem to be a lot of exceptions which are left as an exercise for the reader to figure out.

Example 65 Things that can go wrong:

1. Intersections may occur at infinity, or at complex points. Example: two circles seem to have at most 2 intersection points. Other are at ( $1: \pm i: 0)$. Solution: use projective space.
2. Curves may have a component in common. Solution: exclude this. Not so easy to deal with in higher dimensions: for example, 3 planes in $P^{3}$ might meet in a line.
3. Curve may have a singularity with multiplicity ¿1. Can either exclude these or count points with multiplicities.
4. Curves may intersect non-transversely. Can either exclude these or count points with multiplicities.

Problem: how does one define multiplicity of intersection of 2 curves? Example: $y^{3}-x^{4}$ and $y^{5}-x^{6}$ : not obvious what the intersection multiplicity is. Can try to deform curves slightly to get intersection multiplicities 1. "What is true up to the limit is true at the limit".

Example 66 How many lines intersect 4 lines in $P^{3}$ ? Expect a finite number, as this is intersection of 4 hypersurfaces in 4-dim Grassmannian $G(2,2)$. Guess solution as follows: degenerate lines so they meet in 2 pairs. Then there are 2 lines meeting all 4: line joining 2 intersection points, and intersection of 2
planes. Problem: make this rigorous! (Schubert calculus = cohomology ring of Grassmannian $=$ Littlewood-Richardson coefficients.)

Theorem 62 distinct irreducible curves in $P^{2}$ of degrees $m$, $n$ intersect in mn points, counted with multiplicities.

Problem: define multiplicity. Solution: prove theorem, define multiplicity to be what is needed to make proof work! It will turn out to be dim (local ring $/(f, g)$ ). (Reality check: this is 0 if $f$ or $g$ does not vanish, and 1 if curves of $f, g$ intersect transversely without multiple points. Also depends only on completion $\bmod f, g$, so really is a local invariant.)

To prove theorem, calculate degree of intersection in 2 different ways. Intersection is given by ideal, and is a closed subscheme rather than a subvariety.

## 2 Schemes

Schemes generalize algebraic sets: need not be over fields, and need not be reduced. Affine algebraic sets correspond to finitely generated algebras over a field with no nilpotents: affine schemes correspond to any commutative rings.

### 2.1 Sheaves

Invented by Leray around 1950. Grauert's comment on the work of Cartan and Serre: "We have bows and arrows, the French have tanks". Introduced into algebraic geom by Serre in FAC.Motivation for sheaves and cohomology: cleans up algebraic geom and makes it rigorous. Typical example: old definition of arithmetic genus for a surface in $P^{3}$ is

$$
p_{a}=\binom{\mu_{0}-1}{2}-\left(\mu_{0}-4\right) \varepsilon_{0}+\varepsilon_{1} / 2-\varepsilon_{0}+2 t
$$

where $\mu_{0}$ for example is the degree of the section of the surface by a hyperplane, and the other invariants are defined similarly. Arithmetic genus and irregularity are invariant of the surface, independent of embedding. This was very mysterious, and it was unclear how to generalize this to higher dimensions. In terms of sheaf theory, arithmetic genus is essentially the Euler characteristic, and irregularity is dim of $H^{1}$. Trivial to generalize in higher dimensions: Hodge numbers $h^{p q}=\operatorname{dim} H^{q}\left(\Omega^{p}\right)$.

Let $X$ be a topological space. For each open $U \subseteq X$ put $\mathcal{F}(U)=$ continuous functions on $U$. Then whenever $V \subseteq U$ we have a restriction morphism $\rho_{\mathrm{UV}}$ : $\mathcal{F}(U) \rightarrow \mathcal{F}(V)$. This satisfies

1. $\rho_{U U}$ is the identity map
2. $\rho_{\mathrm{UW}}=\rho_{\mathrm{VW}} \circ \rho_{\mathrm{UV}}$

In other words, we have a contravariant functor from the category of open sets to the category of groups, or a presheaf of abelian groups.

In addition suppose that $U_{i}$ is a cover of $U$. then

1. If the restriction of $s, t \in \mathcal{F}(U)$ to all $U_{i}$ are same, then $s=t$. (This implies $\mathcal{F}(\varnothing)$ has at most 1 element).
2. If we are given $s_{i} \in U_{i}$ whose restrictions to $U_{i} \cap U_{j}$ are the same, then there is some $s$ with restrictions $s_{i}$. (Unique by condition 1.)

$$
\mathcal{F}(U) \rightarrow \prod \mathcal{F}\left(U_{i}\right) \rightrightarrows \prod \mathcal{F}\left(U_{i} \cap U_{j}\right) \text { exact }
$$

A presheaf satisfying these conditions is called a sheaf. Morphisms of presheaves or sheaves are just natural transformations of functors. Sheaves form full subcategory of presheaves.

More generally we can define a presheaf with values in any cat over any cat as a contravariant functor. Most important cases are sheaves of sets and sheaves of abelian groups. If the base cat has a Grothendieck topology (describes covering families) then we can define sheaves. Philosophy of sheaves: the sheaves over a top space form a weak model of set theory, in the sense that any constructive operations on sets can be done on sheaves. More precisely they form a topos. Similarly sheaves of abelian groups behave very much like abelian groups (they are the "abelian groups" of the category of sheaves). For example, sheaves of abelian groups form an abelian category with tensor products.

Example 67 Sheaves of continuous/smooth/analytic/holomorphic functions, or regular functions on a variety.

Example 68 Skyscraper sheaf: $\mathcal{F}(U)=A$ if $p \in U, 0$ otherwise.
Example 69 If $f: Y \rightarrow X$ put $\mathcal{F}(U)=$ continuous sections of $f$ over $U$ to get a sheaf. For example this gives the sheaf of a vector bundle. In fact any sheaf can be obtained like this from the etale space of $\mathcal{F}$. Construction of etale space of a presheaf is as follows: define stalk of $\mathcal{F}$ at $p$ to be $\lim _{\rightarrow p \in U} \mathcal{F}(U)$. Etale space is the union of the stalks with following topology. Base of open sets given by taking any open $U$ and any $s \in \mathcal{F}(U)$ and taking image of $s$ at all stalks of $U$. This makes projection into an etale map: every point of etale space has an open neighborhood mapped homeomorphically to its image. Put $\mathcal{F}^{+}(U)=$ sections of etale space over $U$. Then if $\mathcal{F}$ is a sheaf, $\mathcal{F}=\mathcal{F}^{+}$. More generally, any map from $\mathcal{F}$ to a sheaf factors through the sheaf $\mathcal{F}^{+}$in a unique way: this is the universal sheaf generated by the presheaf.

Example 70 If $A$ is a discrete group, define constant presheaf and constant sheaf. Note that these are DIFFERENT in general.

Suppose $f: X \rightarrow Y$ is a continuous map of top spaces. There are 2 fundamental operations: $f_{*}$ taking sheaves on $X$ to sheaves on $Y$ defined by
$f_{*}(\mathcal{F})(V)=\mathcal{F}\left(f^{-1}(V)\right)$, and $f^{-1}$ in other direction given by pullback of etale space. The functor $f^{-1}$ is left adjoint to $f_{*}$ : maps $f^{-1} \mathcal{G} \rightarrow \mathcal{F}$ are "same as" maps $\mathcal{G} \rightarrow f_{*}(\mathcal{F})$.(Left adjoints are in practice often the "free" object while right adjoints often "forgetful"; for example free group on a set is left adjoint to forgetful functor from groups to sets.)

Now suppose $X$ and $Y$ are ringed spaces (spaces with a sheaf of rings) and suppose that $f$ is a morphism of ringed spaces. Then if $\mathcal{G}$ is a sheaf of $\mathcal{O}_{Y}$ modules, $f^{-1} \mathcal{G}$ is a sheaf of $f^{-1} \mathcal{O}_{Y}$ modules but need not be a sheaf of $\mathcal{O}_{X}$ modules, so define $f^{*} \mathcal{G}=f^{-1} \mathcal{G} \otimes_{f^{-1} \mathcal{O}_{Y}} \mathcal{O}_{X}$. Then $f^{*}$ is left adjoint to $f_{*}$ considered as functors between cats of modules.

A fundamental problem is to determine when a map of sheaves is injective or surjective or an isomorphim. For injective maps this is straightforward a map of sheaves is injective if and only if the maps of stalks are injective, and this is in turn equivalent to the maps of sections being injective. For surjective maps things are more subtle. It is still true that a map is surjective if and only if the maps of stalks are surjective. However if a map of sheaves is surjective, this does NOT imple that the corresponding maps of sections are surjective. The fundamental example is the fact from complex analysis that the logarithm function cannot be defined everywhere on the nonzero complex numbers: in terms of sheaves this means that although the map of sheaves

$$
0 \rightarrow 2 \pi i Z \rightarrow O \rightarrow O^{*} \rightarrow 0
$$

is exact, the corresponding map of sections is NOT surjective on the right: for example there is no global function "log" mapping to $x$, even though such a function can be defined locally everywhere. This lack of surjectivity is fundamental in algebraic geometry, and is the cause of cohomology theory, which is a way of controlling the lack of exactness. More precisely for any exact sequence

$$
0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0
$$

of sheaves we get the corresponding long exact sequence of cohomology groups.
Sheaves are a sort of generalization of vector bundles, which are in turn a twisted generalization of trivial vector bundles. One difference between a sheaf and a vector bundle is that sheaves may have support on a closed subset: for example, if V is the vector bundle whose sections are smooth functions on R , and $x$ is multiplication by $x$, then the map $x$ from $V$ to $V$ is a surjection as a map of vector bundles but not as a map of sheaves: quotient is a skyscraper sheaf at 0 that cannot be detected by vector bundles. In more technical terms, vector bundles form a category that is additive but not abelian, while abelian sheaves form an abelian category.

Example: the map from the 1-dimensional vector bundle to itself over $R$ given by multiplication by $x$ has cokernel a skyscraper sheaf at 0 , not corresponding to a vector bundle.

### 2.2 Schemes

Several experiments with generalizing algebraic sets in the 1950s by Chevalley, Serre, Grothendieck produced schemes as the most powerful. (Named first used by Chevalley.) There are also many suggestions for generalizing schemes: algebraic spaces, locally ringed toposes, stacks (Janos Kollar "Their study is strongly recommended to people who would have been flagellants in earlier times"), noncommutative algebraic geometry.

Affine schemes are locally ringed spaces $\leftrightarrow$ commutative rings; scheme is called Spectrum of the ring $\operatorname{Spec}(\mathrm{R})$. Scheme is a locally ringed space looking locally like an affine scheme, just as a quasiprojective variety looks locally like affine variety.

Reason for name "spectrum": Spectrum of an operator $A$ is set of eigenvalues $=$ homomorphisms from $\boldsymbol{C}[A] \rightarrow \boldsymbol{C}=$ maximal ideals of the ring $\boldsymbol{C}[A]$. Same if $A$ is a set of commuting operators on a complex vector space. This is the finite dimensional case. Now look at a compact Hausdorff space $X$ and $C(X)$. How to reconstruct $X$ from $C(X)$ ? A. $X$ is the set of max ideals of $C(X)$ (if an ideal does not vanish at any point, we can find a function in it that is positive everywhere by taking a sum of squares). Topology given by closed sets=max ideals containing some ideal. Maximal spectrum of commutative $C^{*}$ algebra $=$ set of max ideals with topology. Similarly max ideals of coordinate ring of algebraic set over $\boldsymbol{C}=$ points of algebraic set. This suggests we look at maximal spectrum $=$ max ideals of any commutative ring. Problem: suppose $f: R \rightarrow S$. We would like this to induce a map from $\mathrm{Spec}_{m} S \rightarrow \mathrm{Spec}_{m} R$. However inverse image of a max ideal need not be a max ideal, as subring of a field need not be a field. Most we can say about it is that it is an integral domain. Inverse of a prime ideal is a prime ideal, as subring of int domain is int domain, so PRIME SPECTRUM of a ring is a contravariant functor.

Topology on $\operatorname{Spec}(R)$ : Closed sets $=$ prime ideals containing given set (or ideal). Base of open sets given by $D(f)=$ prime ideals not containing $f$. Key point: work with open sets $D(f)$ rather than with arbitrary open sets.

Weird properties: not only is $\operatorname{Spec}(R)$ not Hausdorff, but it may have points that are not closed! In fact, closed points are exactly the maximal ideals.
(Remark: maximal ideals of $C(X)$ for $X$ compact Hausdorff are just points but the prime ideals can be rather weird: for example, pick a sequence, and take functions vanishing on an element of some ultrafilter. Don't try to mix alg geom and analysis.)

Example $71 \operatorname{Spec}($ field $)=$ point. $\operatorname{Spec}(Z)=$ primes with 0 . (0) is not a closed point! $\operatorname{Spec}(\boldsymbol{C}[x])$ similar: affine line + extra generic point. $\operatorname{Spec}(\boldsymbol{C}[x, y])$ has points of plane + generic points of irreducible curves+generic point for whole space. Spec of discrete valuation ring has 2 points, one closed. Spec $k[x, y]$ localized at $(x, y)$ or at $(f(x, y))$. Spec $k[x, y] /(f(x, y))$.

Example $72 \operatorname{Spec}(\boldsymbol{Z}[x])$ Fibered over $\operatorname{Spec}(\boldsymbol{Z})=(0),(2),(3),(5), \ldots$ Fiber over $(p)$ is spectrum of $F_{p}[x]$ which consists of 0 (closure $=$ fiber) and irre-
ducible polynomials over $F_{p}=$ orbits of alg closure under Galois group (Frobenius) (closed points). Fiber over 0 is $\operatorname{Spec}(\boldsymbol{Q}[x])=0$ (generic: closure=whole space) plus irreducible polynomials over $Q=$ orbits of alg numbers under absolute Galois group of $\boldsymbol{Q}=$ content free irreducible polynomials over $\boldsymbol{Z}$ with positive leading coefficient (closure $=$ union of reduction $\bmod p$ for all $p$ ). So describing $\operatorname{Spec}(\boldsymbol{Z}[x])$ requires all of alg number theory. DIAGRAM: draw closures of $\left(x^{2}+1\right),(x-5)$ which intersect in 2 points. $\operatorname{Spec}(\boldsymbol{Z}[x])$ is 2-dimensional, and behaves like an algebraic surface.

Example 73 Nagata counterexample to almost everything: an infinite dimensional Noetherian affine scheme. In the ring $k\left[x_{1}, \ldots\right]$ consider the primes ideals $\left(x_{1}\right),\left(x_{2}, x_{3}\right),\left(x_{4}, x_{5}, x_{6}\right), \ldots$ and let $R$ be the ring given by inverting all elements not in any of these ideals. Then ideals generated by these elements are exactly the max ideals of $R$. Any prime ideal is generated by irreducibles so by elements with variables in just one of these subsets. So all prime ideals are finitely generated and ring is Noetherian (Cohen). We have a map from $R$ to $R_{\mathfrak{m}}$ embedding $\operatorname{Spec}\left(R_{\mathfrak{m}}\right)$ as subset of $\operatorname{Spec} R$, and these intersect only in 0 and have union $\operatorname{Spec} R$. Describe $\operatorname{Spec} R_{m}$. On the other hand ring is infinite dimensional as it has arbitrarily long chains of prime ideals $\left(x_{n}\right) \subset\left(x_{n}, x_{n+1}\right) \subset \ldots$. Noetherian local rings all finite dimensional: dim at most number of generators of max ideal.

Variation: a 1-dim integral domain with all closed points singular. Take subring generated by $x_{i}^{2}, x_{i}^{3}$ for all $i$, and invert anything not in one of the prime ideals $\left(x_{i}^{2}, x_{i}^{3}\right)$. This forces these ideals to be the maximal ideals. All local rings at these points are singular, given by local ring of a cusp over a field of infinite transcendence degree.

Noetherian rings can be quite strange: what is "correct" class of rings of geometrical rings that aviods examples like this? No generally agreed answer; Grothendieck suggested excellent rings.

Basic properties of topological space $\operatorname{Spec}(R)$

1. Every closed irreducible set is closure of a point (and conversely!) If $S$ is a closed set of prime ideals, then it is set of prime ideals containing their intersection $I$. If $I$ is not prime, pick $a, b \notin I, a b \in I$. Then $S$ is union of primes containing $(I, a)$ and $(I, b)$ so is not irreducible. So if $S$ is irreducible then $S$ is closure of prime ideal $I$.
2. Space is ALWAYS compact (if a set of elements generates the unit ideal, then some finite subset does).

Recall localization $R_{S}$ of $R$ at a multiplicative set $S=$ ring generated by adjoining inverses of $S$. Problem: what is kernel of natural map $R \rightarrow R_{S}$ ? Answer: elements of $R$ killed by some element of $S$. Proof: construct $R_{S}$ explicitly as equivalence classes of pairs $(r, s)=r / s$, where $r_{1} / s_{1}=r_{2} / s_{2}$ if $s\left(r_{1} s_{2}-r_{2} s_{1}\right)=0$ for some $s \in S$. If $S$ has no zero divisors can omit $s$ and this is usual construction of rationals.

Now define locally ringed space structure. Recall $D(f)$ form base of open sets. Put $\mathcal{O}(D(f))=R_{f}$.

Key technical lemma for simplifying arguments about sheaves:
Lemma 1 Can define sheaves by defining them on a base for topology and checking sheaf axioms just for coverings by this base.

So we just need to check the sheaf property for covers of $D(f)$ by $D\left(f_{i}\right)$. By replacing $R$ by $R_{f}$ can assume $f=1$ so have to check for a cover of $\operatorname{Spec}(R)$ by sets $D\left(f_{i}\right)$. This means $f_{i}$ generate unit ideal, so some linear combination of a finite number is $1=a_{1} f_{1}+\ldots+a_{n} f_{n}$.

First do easy check that $r$ is determined by its restrictions: if $r=0$ when restricted to $D\left(f_{i}\right)$ then $f_{i}^{n_{i}} r=0$ for some $n_{i}$. Can replace $f_{i}$ by any power, so can assume $n_{i}=1$ so $r f_{i}=0$. But then $r=r 1=r a_{1} f_{1}+\ldots=0$.

Hard part is to show that compatible elements $r_{i} / f_{i}^{n_{i}}$ on $D\left(f_{i}\right)$ lift to some $r \in R$. Compatibility condition says $f_{i}^{m_{i}} f_{j}^{m_{j}}\left(r_{i} f_{j}^{n_{j}}-r_{j} f_{i}^{n_{i}}\right)=0$ for some $m$ 's. As before we can replace $f_{i}$ by some high power to assume that all $m$ 's and $n$ 's are 1 . So we have elements satisfying

$$
\begin{aligned}
& 1=a_{1} f_{1}+\ldots a_{n} f_{n} \\
& 0=f_{i} f_{j}\left(r_{i} f_{j}-r_{j} f_{i}\right)
\end{aligned}
$$

and we want to find $r$ with $r=r_{i} / f_{i}$ in $D\left(f_{i}\right)$, which will follow if $r$ satisifies

$$
0=f_{i}\left(f_{i} r-r_{i}\right)
$$

Now replace $r_{i} f_{i}$ by $s_{i}$ so that $0=s_{i} f_{j}^{2}-s_{j} f_{i}^{2}$ and we have to solve $f_{i}^{2} r=$ $s_{i}$. Then put $g_{i}=f_{i}^{2}$ so we have $1=b_{1} g_{1}+\ldots$ for some $b_{i}, s_{i} g_{j}=s_{j} g_{i}$ and we have to solve $g_{i} r=s_{i}$. But now we can just put $r\left(=b_{1} g_{1} r+\ldots\right)=b_{1} s_{1}+\ldots$ and check that $g_{i} r=g_{i} b_{1} s_{1}+\ldots=g_{1} b_{1} s_{i}+\ldots=s_{i}$.

Stalk of sheaf at a prime $\mathfrak{p}$ is direct limit of $R_{f}$ for $f \notin \mathfrak{p}$ which is local ring $R_{\mathfrak{p}}$. (Hartshorne does things backwards: uses local rings to define sheaf, then checks values on $D(f)$.)

Problem: what does $\mathcal{O}(U)$ look like for other open sets $U$. Correct answer: who cares?

Morphism of schemes $=$ morphism of LOCALLY ringed space. (Recall that this means we need the extra condition that inverse of a maximal ideal of a local ring is in the maximal ideal: geometrically this coresponds to saying that if a functioin vanishes at a point, then its pullback vanishes on the inverse images of this point.) Example of a morphism of ringed spaces that is not a morphism of locally ringed spaces: $R=\mathrm{DVR}$ with quotient field $K$, then map $\operatorname{Spec} K \rightarrow \operatorname{Spec} R$ with image the CLOSED point of $\operatorname{Spec} R$, with map $R \rightarrow K$ given by the inclusion. This is not local, as it does not map the max ideal of $R$ into the max ideal of $K$.

Morphisms between affine schemes correspond to homomorphisms of rings: affine schemes is opposite cat of commutative rings. (As we have just seen, this is FALSE for morphisms of ringed spaces: we need to use morphisms of locally
ringed spaces.) More generally, if $X$ is any locally ringed space, then morphisms of locally ringed spaces from $\operatorname{Spec}(R) \rightarrow X$ are same as ring homomorphisms from $\mathcal{O}(X) \rightarrow R$. In other words the functor Spec is adjoint to the functor $\mathcal{O}$ : Spec $R$ is a sort of universal locally ringed space generated by the ring $R$.

Proj of a graded ring $S$. Underlying set $=$ homogeneous prime ideals not containing all positive degree elements. Topologize by closed sets $=$ primes containing given homogeneous ideal. For any positive degree element $f$ define $D(f)=$ elements of $\operatorname{Proj}(S)$ not containing $f$, (these form a base for the topology) and define $\mathcal{O}(D(f))=$ degree 0 elements of $S\left[f^{-1}\right]$. The $D(f)$ cover $\operatorname{Spec}(S)$. Homogeneous primes of $S$ not containing $f=$ primes of $S_{f}^{0}$.

Example: what is a point of projective line over a ring? Wrong answers:

1. Union of 2 affine lines. (Correct for fields, fails in general as maps from $X$ to $Y \cup Z$ need not have image in $Y$ or $Z$ if $X$ not a point.)
2. Pair of points not both zero, up to units. (Correct for fields, fails in general: zero divisors, etc.)
3. Pair of elements generating unit ideal, up to units. Still fails for rings with nontrivial invertible modules, though OK for local rings. Point is that $R \oplus R$ can have rank 1 submodules ("lines") that are not free modules.
4. Correct definition: pair of elements of an invertible module, generating all stalks, up to isomorphism.

What are points of $\operatorname{Proj}(S)$ with values in a ring $R$, in other words the morphisms from $\operatorname{Spec}(R)$ to $\operatorname{Proj}(S)$ ? First look at case when $R$ is a field $k$. Then $\operatorname{Spec}(R)$ has just one point, so image is certainly in some affine subset $D(f)$. So we get a morphism $\mathcal{O}(D(f)) \rightarrow R$. But $\mathcal{O}(D(f))=$ degree 0 elements of localization $S_{f}=S[1 / f]$ so morphisms $\mathcal{O}(D(f)) \rightarrow R=$ morphisms from $S_{0} \oplus S_{n} \oplus \ldots \rightarrow R$ taking $f$ to a unit, up to multiplying elements of $S_{n}$ by a unit $(n=\operatorname{deg}(f))$. So points are represented by some homomorphism $S_{0} \oplus S_{n} \oplus \ldots \rightarrow R$ that is not zero on positive degree elements, up to multiplying by units and changing $n$ to some multiple. If $S$ is generated by degree 1 elements, can just take $n=1$.

So points of projective space with values in a field is as expected.
Points with values in a local ring similar: key point is that there is a closed point of $\operatorname{Spec}(R)$ in closure of every other point, so any open set of $\operatorname{Proj}(S)$ containing this point contains whole image of $\operatorname{Spec}(R)$. In other words $\operatorname{Spec}(R)$ has image in one of the open sets $D(f)$ as in the case of fields. Argument for fields gives similar answer: points of projective space represented by ( $a_{0}: \ldots: a_{n}$ ) such that at least one $a_{i}$ is a unit, up to multiplication by units.

Example: $R=$ formal power series in $x$ and $y$. Then $(x: y)$ is a point in projective space of quotient field that is NOT represented by a point with values in $R$. Same for $R=\boldsymbol{Z}[x, y]$

Example: integer valued points of projective space are represented by ( $a_{0}$ : $\left.\ldots: a_{n}\right)$ coprime. Image is NOT usually in one of the open sets $D(f)$ unless some $a_{i}$ is a unit. To see this represents a point, cover $\operatorname{Spec}(\boldsymbol{Z})$ by open subsets
and note that this point is well defined on each open subset and represents the same morphism on intersections.

Example: One might guess from previous examples that points of projective space are represented by $\left(a_{0}: \ldots: a_{n}\right)$ whose elements generate the unit ideal. This is FALSE in general, and related to nonuniquness of factorization in alg number fields: both related to existence of nontrivial invertible modules. Example: $R=\boldsymbol{Z}[\sqrt{-5}]$ Not a UFD as $6=2 \times 3=(1+\sqrt{-5})(1-\sqrt{-5})$, non-principal ideal $=(2,1+\sqrt{-5})$. Look at point $(2: 1+\sqrt{-5})=(1-\sqrt{-5}: 3)$. If we $\operatorname{cover} \operatorname{Spec}(R)$ by open sets $\operatorname{Spec}(R[1 / 2]), \operatorname{Spec}(R[1 / 3])$ then these 2 expressions represent points on the 2 open sets, equal on their intersection. So they give a point of projective space.

Key property of $\operatorname{Proj}(S)$ : there is a special line bundle $\mathcal{O}(1)$ over it. Line bundle $=$ sheaf of modules over $\mathcal{O}$ that is locally isomorphic to $\mathcal{O}$ (locally free of rank 1). Informal picture: associate a 1-dim vector space over residue field at each point. Informal examples: Moebius band, highest exterior power of (co)tangent bundle over smooth manifold. Projective space $=$ set of lines in a vector space, so we can associate this line to each point of projective space. (Similarly Grassmannians have a special vector bundle.) More formal construction: Cover projective space by open affine sets $D\left(x_{i}\right)$. On each of these the line bundle will be trivial, so we can identify it with the ring of regular functions. How do we change in going from $D\left(x_{i}\right)$ to $D\left(x_{j}\right)$ ? A. Multiply by $f_{i j}=x_{i} / x_{j}$ (or $\left(x_{i} / x_{j}\right)^{n}$ ) called transition functions. So a global section of line bundle is given by elements $s_{i}$ of $\mathcal{O}\left(D\left(x_{i}\right)\right)$ such that $s_{j}=s_{i} f_{i j}$ on $U_{i} \cap U_{j}$. (Easy to get this wrong way round!) For example, for projective space, put $s_{i}=x_{j} / x_{i}$, a degree 0 element of $k\left[x_{0}, \ldots, x_{n}, x_{i}^{-1}\right]$, so $x_{j}$ gives a section of this line bundle, and similarly degree $k$ polynomials are sections of $m$ 'th tensor power $\mathcal{O}(m)$. Transition functions have to be invertible in $\mathcal{O}\left(U_{i} \cap U_{j}\right)$ and compatible on $\mathcal{O}\left(U_{i} \cap U_{j} \cap U_{k}\right)$ : $f_{i j} f_{j k} f_{k i}=1$. (A Cech $1=$ cocyle) Warning: in diff geom all vector bundles are isomorphic to their duals as we can find a metric on them, but in alg geom this is completely false and $\mathcal{O}(1)$ is totally different from its dual $\mathcal{O}(-1)$. Warning: For projective space all sections of $\mathcal{O}(m)$ are given by elements of $S_{m}$ but this is not true for general graded rings.

Remark 3 In alg topology, classifying space for complex line bundles over CW complexes is infinite dimensional complex projective space. Chern class = image of generator of 2 nd cohomology of $\mathrm{CP}^{\infty}$; classifies complex line bundles. In algebraic geom line bundles harder to classify: get continuous families.

### 2.3 First properties of schemes

Contains about a gazillion definitions, all important.
Definition 4 Define integral, irreducible, connected, reduced.
Definition 5 Locally Noetherian $=$ covered by Spec of Noetherian ring. Noetherian $=$ locally Noetherian + compact .

Common problem: Does "locally X " mean " has a base of affine X " or "every open affine subset is X". Usually equivalent in practice. Want to show: (1) Localization of X ring is X and (2) If Spec R is covered by (finite number of) X sets $D\left(f_{i}\right)$ then $R$ is $X$. Check these 2 conditions for $\mathrm{X}=$ Noetherian. (1) Localization of Noetherian ring obviously Noetherian. (2) Suppose $R_{f_{i}}$ Noetherian. If $I$ is an ideal of $R$ then we can find a finite set of generators of $I_{f_{i}}$; we can assume these are in $R$, so we have a finite set $\left\{g_{1}, \ldots\right\}$ that generates all $R_{f_{i}}$. We show this generates $I$. We have $r f_{i}^{n_{i}} \in\left(g_{1}, \ldots\right)$ so $r=r 1^{n_{1}+n_{2}+\ldots} \in\left(g_{1}, \ldots\right)$.

Definition $6 f: X \rightarrow Y$ is Locally of finite type if $X$ is covered by affines such that each inverse image is covered by finitely generated affines. Finite type if each inverse image is covered by a finite number of finitely generated affines.

Example: Varieties are finite type as they are covered by a finite number of affine varieties, which are finitely generated algebras. In fact abstract varieties are exactly the schemes that are reduced and integral and of finite type over a field. Hilbert scheme is locally of finite type over a field but not of finite type: infinitely many connected components! Finite type can be thought of vaguely as finite dimensional fibers.

Definition $7 f: X \rightarrow Y$ is quasifinite if inverse image of any point is finite, and finite if it is covered by affines such that inverse image is Spec of a finite algebra (=finite as a MODULE not an ALGEBRA).

Finite is much stronger than quasifinite: example: $R \rightarrow R_{S}$, or any open immersion, is always quasifinite, as inverse image of a point has at most 1 element, but is rarely finite. Finite implies finite type (but quasifinite does not). Examples of finite morphisms: $\operatorname{Spec} A \rightarrow \operatorname{Spec} Z$ for $A$ integers of algebraic number field. Projection from projective curve to $P^{1}$.

Open immersions and finite morphisms are in some sense the only ways to get quasifinite ones. Grothendieck' generalization of Zariski's main theorem: if Y is a quasi-compact separated scheme and $f: X \rightarrow Y$ is a separated, quasifinite, finitely presented morphism then there is a factorization into $X \rightarrow Z \rightarrow Y$ where the first map is an open immersion and the second one is finite.

Stein factorization: proper morphisms of Noetherian schemes can be written as composition of a morphism with connected fibers and a finite morphism. For these morphisms it follows that proper + quasi finite implies finite. (Stein factorization and Zariski's main theorem both follow from Grothendieck's theorem on formal functions, covered in chapter on cohomology.)

Definition 8 Open/closed subschemes. Given by open/closed subsets of scheme such that induced map of sheaves is identity/quotient.

Note that open subschemes are determined by the subset, but closed subschemes are NOT.

Example: A localization $\operatorname{Spec}\left(R\left[f^{-} 1\right] \subseteq \operatorname{Spec}(R)\right.$ is an open immersion. The reduced induced closed subscheme is a closed subscheme. $k[x] /\left(x^{n}\right)$ is a closed subscheme of $k[x]$. Closed subschemes of affine schemes correspond to ideals.

Define pullbacks for categories.
Theorem 7 Fibered products $X \otimes_{S} Y$ (= pullbacks= base extension) exists for schemes.

Proof Requires a lot of tiresome bookkeeping to do properly.
Case 1: everything affine. In category of affine schemes, this is just given by tensor product. Check that this is still a fibered product in cat of all schemes.

Case 2: $S$ affine. Now cover any 2 schemes over an affine $S$ by affines $X_{i} Y_{j}$, and construct fibered product by gluing together $X_{i} \otimes_{S} Y_{j}$.

Case 3: general case. Now suppose $S$ is covered by affines $S_{i}$. Construct $X \otimes_{S} Y$ by gluing together $X_{i} \otimes_{S_{i}} Y_{i}$ where $X_{i}, Y_{i}$ are inverse images of $S_{i}$. (Can also use $\left.X_{i} \otimes_{S_{i}} Y_{i}=X_{i} \otimes_{S} Y\right)$

Warning 3 The scheme product of $X$ and $Y$ over $S$ not only has more open sets than the topological product, but usually has far more points. Example: Spec $k[x] \times_{\text {Spec } k} \operatorname{Spec} k[y]$ has all irreducible curves as extra points.

Example 74 (suggested by Ryan Reich, Pete L. Clark on mathoverflow.net) Fiber products of reduced schemes can be nonreduced. Take pullback of identity map and $p^{\prime}$ th power map of algebraic group $G_{m}=\operatorname{Spec} k\left[x, x^{-1}\right]$ where $k$ has characteristic $p$. Result is $k[x] /\left(x^{p}-1\right)$ (a non-reduced group scheme representing $p^{\prime}$ th roots of 1 ). Or take $K \otimes_{k} K$ where $K$ is an inseparable extension of the field $k$ such as $k[x] /\left(x^{p}-a\right)$. Then tensor product is $k[x, y] /\left(x^{p}-a, y^{p}-a\right)$ so $(x-y)^{p}=0$.

### 2.4 Separated and proper morphisms

Separated is analogue of Hausdorff, proper is analogue of compact (or rather proper). Problem: find definition of these concepts for top spaces that work well for schemes. A. A top space $X$ is Hausdorff $\leftrightarrow$ diagonal is closed in $X \times X$. If $X$ is compact then $X \rightarrow 1$ is universally closed: $X \times Y \rightarrow Y$ is closed for all $Y$. Key point: for schemes we use the scheme product, not the product topology.

Definition 9 A morphism is called SEPARATED if the image of the diagonal is closed.

Example: Any morphism $R \rightarrow S$ of rings gives a separated morphism. Diagonal map corresponds to $R \otimes_{S} R \rightarrow R$ so diagonal is closed subset of $\operatorname{Spec}\left(R \otimes_{S} R\right)$ of prime ideals containing $\operatorname{ker}\left(R \otimes_{S} R \rightarrow R\right)$.

Example: Line with 2 origins (bug eyed line).
Definition 10 A morphism is called PROPER if it is separated of finite type and universally closed.

### 2.4.1 Valuation rings

Recall that a valuation ring is a domain such that for any 2 elements one divides the other. They are all local rings. Valuation group $=$ nonzero elements of quotient field mod units: ordered by divisibility. DISCRETE valuation rings: valuation group $=$ integers. Nondiscrete valuation rings can be strange: any Noetherian valuation ring is a DVR or a field. Example of valuation rings:

1. p-adic numbers
2. Formal power series in 1 variable
3. 1-dim regular local ring. Example: local ring of irreducible curve in nonsingular surface.
4. Puiseux power series; valuation group $=$ rationals. Nondiscrete, height 1
5. Put $v(f)=$ multiplicity of 0 for $f \in k[x, y]$. Then elements of quotient field with $v \geqslant 0$ form a DVR.
6. As above, but give $x, y$ different integral weights.
7. As above, but given $x, y$ IRRATIONAL weights: nondiscrete DVR.
8. Take smooth surface. Repeatedly blow up points on exceptional curve. Union of local rings is a valuation ring (not trivial: need to know this resolved sings of a function.)
9. Ring of formal powers series with exponents the nonnegative elements of a totally ordered group.

The following are equivalent:

1. $R$ is a DVR
2. $R$ is a Noetherian valuation ring other than a field
3. $R$ is a 1-dim regular Noetherian local ring
4. $R$ is a valuation ring and a PID

Spec of a DVR $R$ has 1 closed point and one generic point. Something like a short smooth curve. They tend to be associated to divisors not contained in singular locus: local ring of a hypersurface is a DVR whose valuation measures the order of the zero of a function along the divisor.

Geometric meaning of valuation ring. Zariski defined spaces that were precursors to Spec and Proj. Take extension of fields $k \subseteq K$ where we think of $K$ as rational functions on some variety over $k$. In 1-dim, valuation rings in $K$ containing $k=$ Riemann surface (more or less) $=$ complete nonsingular model of curve. Try to copy this in higher dims: define Zariski-Riemann space $=$ all valuation rings of $K$ containing $k=$ places of $K$ over $k$. (More generally can
use local rings instead of valuation rings). Zariski topology: basis of open sets given by valuation rings not containing given finite set.

Recall spectrum of a DVR has 2 point (0) (open) and $\mathfrak{m}=(p)$ (closed). Stalk at $(0)=$ regular functions on $(0)=$ field of quotients, and stalk at $(p)=$ regular functions on whole space $=R$.

A morphism from $\operatorname{Spec}(R)$ to a scheme $S$ is given by following date:

1. 2 points $a, b$ of $S$ with $a$ in closure of $b$; the images of $(p),(0)$.
2. Maps from the stalks of $a$ and $b$ to $R$ and $K$ that commute with the restriction maps $(R \rightarrow K)$ and map the max ideals into the max ideals.

Theorem 8 Suppose $f: X \rightarrow Y$ is a morphism of Noetherian schemes of finite type. Then $f$ is separated if and only if given

for a DVR $R$ with quotient field $K$ there is at most one diagonal arrow. $f$ is proper if and only if there is always exactly one diagonal arrow.

Meaning: think of Spec $R$ as a short smooth curve with a special point. Then condition says that maps from rest of curve can be extended to point in at most one or exactly one way.

Recall morphisms from a LOCAL ring to projective space $P^{n}$ (over integers) are given by tuples $\left(a_{0}: \ldots: a_{n}\right)$ such that at least one is a unit, up to multiplication by units. In particular if $R$ is a valuation ring, then points of projective space with values in $R$ are same as points with values in quotient field $K$. Key point: if $\left(a_{0}: \ldots: a_{n}\right)$ has elements in $K$ not all 0 , we can divide by the element with smallest valuation to make it a unit, so all other elements are then in $R$.

Corollary: Projective space over the integers is complete.
Application: when is a toric variety complete, when is a map between them proper.

### 2.5 Sheaves of modules

Define sheaf of modules over a sheaf of rings. (Philosophy: sheaves form weak model of intuitionistic set theory, so constructions for rings should work for sheaves of rings.) Sheaves of modules form an abelian category.

Module $M$ over ring $R$ gives a sheaf of modules over Spec $R$ with sections over $D(f)$ given by $M_{f}$. Proof similar to construction of Spec $R$ : need to show these have sheaf property for open sets of the form $D(f)$. Stalk of sheaf at prime ideal $\mathfrak{p}$ is localization $M_{\mathfrak{p}}$ just as for $R$.

Are sheaves of modules over an affine scheme same as modules over the ring? A. No! Sheaves of modules have special property: suppose $A \subseteq B$ are open affine subschemes. Then $M(A)=M(B) \otimes_{\mathcal{O}(B)} \mathcal{O}(A)$, or $M(A)=M(B)_{f}$ if
$\mathcal{O}(A)=\mathcal{O}(B)_{f}$. Sheaves of modules with this extra property are (unfortunately) called quasicoherent. For quasicoherent sheaves, if we know values on some open affine subscheme we know values on all smaller subschemes; in particular quasicoherent sheaves over affine schemes are essentially the same as modules over rings. Example of a sheaf of modules that is not quasicoherent: take a quasicoherent sheaf over affine scheme and just make it 0 on all proper subsets.

Coherent modules: over Noetherian rings these are same as finitely generated modules. Hartshorne uses coherent to mean finitely generated over all rings but this is not standard terminology. Over general rings, $M$ coherent means finitely generated + kernel of any finitely generated free module mapping to $M$ is finitely generated. Automatic for Noetherian rings as any submodule of a finitely generated free module is finitely generated. Reason for extra condition: in general kernels of maps between finitely generated modules need not be finitely generated, for example any non finitely generated ideal is kernel of map between finitely generated modules. So finitely generated modules need not form abelian category, but coherent modules do. A ring is called coherent if it is coherent as module over itself, so all Noetherian rings are coherent. Ring of polynomials in infinitely many variables is coherent but not Noetherian. Easiest to forget about coherence and just use finitely generated modules over Noetherian rings.

Coherent sheaves: quasicoherent sheaves that come from coherent modules. So for affine Noetherian schemes, quasicoherent sheaves are same as finitely generated modules. Example: sheaf of regular functions, sheaf $\mathcal{O}(1)$ over projective space.

Graded module $M$ over graded ring $R$ gives a quasicoherent sheaf whose value on $D(f)$ ( $f$ homogeneous of positive degree) is degree 0 elements of $M_{f}$. Warning: different graded modules $M$ often give same sheaf: in fact if $M$ is changed on a finite number of pieces this does not change the sheaf.

Fundamental difference between sheaves and modules: sheaf of regular functions is not projective in general; in fact there are sometimes not enough projectives. Recall that global sections of $\mathcal{O}(m)$ over projective space $=$ degree $m$ polynomials. These are also same as maps of sheaves $\mathcal{O}(0) \rightarrow \mathcal{O}(m)$ or $\mathcal{O}(k) \rightarrow \mathcal{O}(m+k)$. We have a map $\mathcal{O}^{n+1} \rightarrow \mathcal{O}(1)$ defined by coordinate functions that is surjective on each $D\left(x_{i}\right)$ and therefore surjective, but does not split as there are no maps from $\mathcal{O}(1) \rightarrow \mathcal{O}$. Global section functor of sheaves not right exact: cause of cohomology.

Notice difference between vector bundles in alg and diff geom: in diff geom all vector bundles isomorphic to their duals as we can put a metric on them, but in alg geom $\mathcal{O}(1)$ is quite different from its dual $\mathcal{O}(-1)$ Also vector bundles in diff geom are projective. Serre-Swan theorem: vector bundes over a smooth manifold or affine variety $=$ coherent projective sheaves; this completely fails for projective varieties.

Discuss free/stably free/projective/flat/torsion free
Free and stably free: example of a stably free module that is not free is the tangent space of a 2-sphere: not free by hairy sphere theorem, stably free as adding normal bundle makes it free. Algebraically we work over the ring $\boldsymbol{R}[x, y, z] /\left(x^{2}+y^{2}+z^{2}-1\right)$ and the tangent bundle $T$ is the submodule of $R^{3}$
of elements $(a, b, c)$ with $x a+y b+z c=0$. An isomorphism from $R^{3} \rightarrow T \oplus R$ takes $(A, B, C) \rightarrow(A-x D, B-y D, C-z D), D$ where $D=x A+y B+z C$.

Compare stably free and projective. Stably free modules are obviously projective as any direct summand of a free module is projective. Note we cannot allow infinitely generated free modules in the definition of stably free as for any projective $P$ there is a free module $F$ with $P \oplus F=F$ : take $F=P \oplus Q \oplus P \oplus Q \oplus \ldots$ where $P \oplus Q$ is free, and use the Eilenberg swindle. Example of a projective that is not stably free: Moebius band over circle (cant get rid of reveral of orientation by adding free bundles), many other vector bundles, non-principal ideals over Dedekind domains such as $(2,1+\sqrt{-5})$ over $\boldsymbol{Z}[\sqrt{-5}]$. It is usually hard to distinguish free and stably free modules: Serre's question asked whether every projective=stably free module over $k\left[x_{1}, \ldots x_{n}\right]$ is free (this is easy to prove for topological vector bundels over real affine space). Solved positively by Quillen and Suslin.

Although free modules are projective, it is NOT true that free sheaves are projective! In fact most schemes have very few projective sheaves. Example: for the variety $P^{1}$, the map from $\mathcal{O}(0) \oplus \mathcal{O}(0) \rightarrow \mathcal{O}(1)$ is surjective, but there are no maps from $\mathcal{O}(1) \rightarrow \mathcal{O}(0)$, so $\mathcal{O}(1)$ is not projective. Twisting by $\mathcal{O}(-1)$ shows that the free module $\mathcal{O}(0)$ of rank 1 is not projective either. In general there are not enough projective sheaves to form projective resolutions, though there are enough injective sheaves.

Warning 4 Vector bundles over schemes or varieties behave differently from topological vector bundles over smooth manifolds. For example, over smooth manifolds, vector bundles are always self dual, because we can put a positive definite bilinear form on them using a partition of unity, but over algebraic projective space the dual of $\mathcal{O}(1)$ is $\mathcal{O}(-1)$. Over smooth manifolds the spaces of smooth sections of vector bundles are flat modules over the ring of smooth functions, but the analogue of this for algebraic vector bundles is false. Over smooth vector bundles exact sequences of bundles split (use positive definite inner product again) but this is completely false for bundles over projective space.

Projective and flat modules: Projectives are flat because any direct summand of a flat module is flat. Examples of flat modules that are not projective: the module $\boldsymbol{Q}$ over $\mathbf{Z}$. Finitely generated flat modules $M$ over a Noetherian local ring $R$ are projective and even free: choose a map $0 \rightarrow K \rightarrow R^{n} \rightarrow M \rightarrow 0$ that is an isomorphism when reduced $\bmod \mathfrak{m}$. Then since $\operatorname{Tor}_{1}(M, R / \mathfrak{m})=0$, we have $K=K \mathfrak{m}$. Since $K$ is finitely generated, Nakayama's lemma implies that $K=0$. (Proof of Nakayama: We have $g=A g$ for some matrix $A$ with coefficients in $\mathfrak{m}$ where $g$ is a vector of generators of $M$, and $\operatorname{det}(1-A)$ is a unit, so $1-A$ is invertible.) So over locally Noetherian schemes, finitely generated flat sheaves correspond roughly to "vector bundles" as they are free over local rings.

Example 75 Classify vector bundles over $P^{1}$. (Grothendieck.) Over $A^{1}$ all
vector bundles are free (coordinate ring is a PID). So cover $P^{1}$ by 2 copies of $A^{1}$ on each of which vector bundle is free of rank $n$. Transition functions are given by an $n \times n$ matrix with coordinates in $k\left[x, x^{-1}\right]$. We can multiply on left by an invertible mattrix in $k[x]$ and on right by invertible matrix in $k\left[x^{-1}\right]$. Using these operations we can make transition matrix $M$ diagonal with entries powers of $x$ as follows. Use operations to make 1 column zero except for one element, necessarily of the form $x^{r}$, and choose $r$ as large as possible, and take this element to be in top left corner. (To show that such a maximal $r$ exists, observe that it is bounded above by integers $t$ such that for some nonzero vector $v$ with coefficients in $k\left[x^{-1}\right], M v$ has all coefficients divisible by $x^{t}$, and this $t$ is invariant under the matrix operations on the left and right, and is bounded by the highest power of $x$ appearing in $M$.) Then by induction we can make matrix diagonal except for top row. Then using maximality of $r$ we can clear top row, using column operations to clear out powers of $x$ that are at most $r$, and row operations to clear out poers that are at least $s$ where $x^{s}$ is the diagonal power in this column. So if there are any entries left in the top row we must have $r<s$ contradicting maximality of $s$. So vector bundle splits as the sum of one dimensional bundles of the form $\mathcal{O}(m)$. Number of copies of $\mathcal{O}(k)$ is uniquely determined by looking at dimensioin of space of sections of bundle twisted by line bundles.

Example: is the matrix $M$ is $\left(\begin{array}{cc}1 & x \\ & x^{2}\end{array}\right)$ then it cannot be turned into the diagonal matrix $\left(\begin{array}{cc}1 & \\ & x^{2}\end{array}\right)$; instead it gets transformed into $\left(\begin{array}{ll}x & \\ & x\end{array}\right)$. This shows we need to take $r$ maximal in the above argument. This corresponds to the fact that the exact sequence $0 \rightarrow \mathcal{O}(0) \rightarrow \mathcal{O}(1) \oplus \mathcal{O}(1) \rightarrow \mathcal{O}(2) \rightarrow 0$ does not split. So although any vector bundle is a sum of line bundles, it can be tricky to find such a decomposition: one cannot just pick sub line bundles at random.

This classification is misleadingly simple: in this case all vector bundles are sums of irreducibles, all irreducibles are 1-dimensional, and irreducibles form a discrete set, none of which are true in general. Over other curves vector bundles are quite hard to classify, and classifying them over varieties of dimension $¿ 1$ is a very difficult open problem, even for projective spaces. Example: HorrocksMumford rank 2 bundle on $P^{4}$.

Flat and torsion free: Any flat module is torsion free (multiplication by non zero divisor is injective) as follows by taking tensor product with $0 \rightarrow R \rightarrow{ }^{a} R$. Torsion free module that is not flat: look at submodule $M$ of $k[x, y]$ generated by $x$ and $y$. Then $\operatorname{Tor}_{1}^{k[x, y]}(M, k)=k$ so $M$ is not flat, but is a submodule of a torsion free module so is torsion free.

### 2.6 Divisors

Divisors on a compact Riemann surface. A divisor $D$ is a finite linear combination of points with integer coefficients: free abelian group with basis the Riemann surface. Degree $=$ sum of coefficients. A meromorphic function has
a divisor of zeros, of degree 0 because \#zeros-\#poles=change in argument. 2 divisors equivalent if difference is divisor of a meromorphic function.

Divisor classes - ¿ line bundles
Riemann Roch. $H^{0}(X, \mathcal{O}(D))=$ space of functions whose only poles are along $D$.
$H^{1}(X, \mathcal{O}(D))=$ space of obstructions to finding a function with given singular parts, except that we only don't care about singularities of order less than $n$ at the point $x$ if $D=\mathrm{nx}+\ldots$.

Then $\operatorname{dim} H^{0}(X, \mathcal{O}(D))-\operatorname{dim} H^{1}(X, \mathcal{O}(D))=\operatorname{deg} D+1-g$ where $g=$ $\operatorname{dim} H^{1}(X, \mathcal{O})$ is the genus. Proof: trivial for $D=0$. Adding a point to $D$ increases $H^{0}$ by 1 if there is a function with a singularity of the appropriate order at this point. If there is not then $H^{1}$ is decreased by 1 . So in either case the left hand side increases by 1. (Nontrivial point: show $H^{1}$ has finite dimension.)

Roch's part: $H^{0}\left(X . \mathcal{O}(-D) \times H^{1}(X, \mathcal{O}(K-D)) \rightarrow \boldsymbol{C}\right.$ given by sum of residues is a perfect pairing. Generalized by Serre duality. $K=$ canonical class $=$ zeros of a meromorphic 1 -form; gives a well defined divisor class. Combining these gives usual RR theorem:
$\operatorname{dim} H^{0}(X, \mathcal{O}(D))-\operatorname{dim} H^{0}(X, \mathcal{O}(K-D))=\operatorname{deg} D+1-g$
Exercise: show $\operatorname{deg} K=2 g-2$.
Picard variety.
Weil divisor: analogue of divisor of a Riemann surface.
Total quotient ring $K$ of a ring $R$ : invert all non zero divisors. $R \subseteq K$. Problem: when does this give a sheaf? Easy if $R$ is integral domain, as then any open subset has sections $K$. Hartshorne cheats slightly by simply taking the sheaf associated to this presheaf, but this loses control of it. Vital principal: keep track of values of a sheaf on (a basis of) open affine sets. We show that associated sheaf has same values as presheaf on open affines for Noetherian schemes. Suppose $\operatorname{Spec}(R)$ is covered by open set $D\left(f_{i}\right)\left(1=a_{1} f_{1}+\ldots\right)$ and we have sections $a_{i} / b_{i}$ where $b_{i}$ is not a zero divisor in $R_{f_{i}}$. Can assume $a_{i} b_{j}=a_{j} b_{i}$ by multiplying by powers of the $f$ 's. Then $b_{i}$ is not a zero divisor in $R_{f_{i}}$ so anything killing $b_{i}$ is killed by a power of $f_{i}$. Want to find $A, B$ with $A b_{i}=B a_{i}$. Let $I$ be ideal of elements such that $I a_{i} \subseteq R b_{i}$ for all $I$, so that $I$ contains all $b$ 's and therefore has no annihilator (as any annihilator is killed by a power of any $f$ and therefore killed by 1 , as the $f$ generate the unit ideal). We want to show that $I$ has a non zero divisor $B$. Now use the fact that $R$ is Noetherian so we have a good theory of associated primes. If every element of $I$ is a zero divisor then $I$ is in the union of the associated primes of $R$, which are finite in number. But any ideal contained in a finite union of primes is contained in one of them (prime avoidance: if $a_{i}$ not in $P_{i}$ but in the others then $a_{1}+a_{2} a_{3} \ldots a_{n}$ not in any) so $I$ is contained in some associated prime of $R$ and therefore kills some nonzero element of $R$, contradiction.

Cartier divisor: sheaf theoretic. Sections of $K^{*} / \mathcal{O}^{*}$. Cartier divisors $\subseteq$ Weil divisors. Same as Weil on integral separated Noetherian schemes such that local rings are UFDs (e.g. regular: deep theorem). Nonregular local rings not UFDs in general, example $k\left[\left[x^{2}, x^{3}\right]\right]$. Example of a nonregular local ring that is a

UFD: $R=k[x, y, z] /\left(x^{2}+y^{3}+z^{5}\right)$ is a UFD, so its localization at 0 is as well. Proof: The subring $k\left[x / z^{3}, y / z^{2}\right]$ is a UFD as it is a polynomial ring, and it contains $z^{-1}$. So its localization at $z^{-1}$ is a UFD and is the same as $R\left[z^{-1}\right]$. Now check that $z$ is a prime of $R$. Since $z$ is a prime and $R\left[z^{-1}\right]$ is a UFD, $R$ is also a UFD.

### 2.7 Projective morphisms

### 2.8 Differentials

### 2.9 Formal schemes

