These are cleaned up notes for the lectures on 2/20, 2/25, and 2/27.

Philosophy is done ^_^
Now we need some details.

The goal is to discuss integral ring extensions, so we can prove at least one or two theorems of Algebraic Geometry.

Definition: Let $R \subseteq S$ be an extension of commutative rings (this is just a fancy way to say that R is a subring of S). Then given any $\alpha \in S$ we define the evaluation map

$$ev_\alpha : R[x] \longrightarrow S$$

by $ev_\alpha\left(\sum a_k x^k\right) := \sum a_k \alpha^k \in S$

It is easy to see that this is a ring homomorphism. In fact we defined $R[x]$ so that this would be the case.

To simplify notation we write

$$ev_\alpha(f(x)) = \text{“}f(\alpha)\text{”}.$$

We can say this more formally as follows

✡ Evaluation Theorem: We have a bijection

elements of $S \longleftrightarrow$ ring homs $R[x] \to S$ that fix R.

Proof: The bijection is $\alpha \longleftrightarrow ev_\alpha$.

Given $\alpha \neq \beta$ in S note that $ev_\alpha \neq ev_\beta$ because $ev_\alpha(x) = \alpha \neq \beta = ev_\beta(x)$.

Now let $\varphi : R[x] \to S$ be any ring hom such that $\varphi(a) = a$ for all $a \in R$, and define $\alpha := \varphi(x) \in S$. Then for all $\sum a_k x^k \in R[x]$ we have

$$\begin{aligned} \varphi\left(\sum a_k x^k\right) &= \sum \varphi(a_k x^k) \\ &= \sum \varphi(a_k)\varphi(x)^k \\ &= \sum a_k \alpha^k \\ &= ev_\alpha\left(\sum a_k \alpha^k\right), \end{aligned}$$

hence $\varphi = ev_\alpha$ ///

[This allows us to think about polynomials as "functions".]

Notation: We define

$$R[\alpha] := \mathrm{im}(ev_\alpha)$$

$$= \{ f(\alpha) : f(x) \in R[x] \} \subseteq S.$$

Theorem: $R[\alpha]$ is the smallest subring of S containing R and α.

Proof: Clearly $R[\alpha]$ is a subring of S that contains R and α.

Now suppose $T \subseteq S$ is any other subring containing R and α. Then for all $f(x) = \sum a_k x^k \in R[x]$ we have

$$ev_\alpha(f(x)) = f(\alpha) = \sum a_k \alpha^k \in T,$$

hence $R[\alpha] = \mathrm{im}(ev_\alpha) \subseteq T$. ///

We call $R[\alpha]$ = "R adjoin α"

We will be concerned with properties of $R[\alpha]$ as an R-module. In particular, we want to know when $R[\alpha]$ is finitely generated as an R-module.

Definition: Given a ring extension $R \subseteq S$ we say that $\alpha \in S$ is integral over R if there exists a monic polynomial $f(x) \in R[x]$ such that

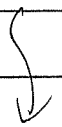
$$f(\alpha) = 0.$$

"integral" = "root of a monic polynomial"

Example: The golden ratio

$$\phi = (1+\sqrt{5})/2 \in \mathbb{R}$$

is integral over $\mathbb{Z}$ because



$$2\phi = 1+\sqrt{5}$$
$$2\phi - 1 = \sqrt{5}$$
$$4\phi^2 - 4\phi + 1 = 5$$
$$4\phi^2 - 4\phi - 4 = 0$$

and $x^2 - x - 1 \in \mathbb{Z}[x]$ is monic. //

However, the closely related

$$\alpha = (1+\sqrt{3})/2$$

is not integral over $\mathbb{Z}$.

How can we prove this ??

We must show that there does not exist a monic polynomial $f(x) \in \mathbb{Z}[x]$ with $f(\alpha) = 0$.

It helps to work over the field

$$\mathbb{Q} = \text{Frac}(\mathbb{Z})$$

Consider the evaluation map

$$ev_\alpha : \mathbb{Q}[x] \longrightarrow \mathbb{R}$$

Since $\mathbb{Q}$ is a field, $\mathbb{Q}[x]$ is a PID and we have

$$\ker(ev_\alpha) = (m_\alpha(x))$$

for some $m_\alpha(x) \in \mathbb{Q}[x]$ called the minimal polynomial of α over $\mathbb{Q}$

[This $m_\alpha(x)$ is unique if we assume that its leading coefficient is 1, which we will.]

How can we compute $m_\alpha(x)$? Note that

$$\alpha = (1+\sqrt{3})/2$$
$$2\alpha = 1+\sqrt{3}$$
$$2\alpha - 1 = \sqrt{3}$$
$$4\alpha^2 - 4\alpha + 1 = 3$$
$$4\alpha^2 - 4\alpha - 2 = 0$$
$$2\alpha^2 - 2\alpha - 1 = 0.$$

Let $f(x) := 2x^2 - 2x - 1 \in \mathbb{Q}[x]$. Then

$$f(\alpha) = 0$$
$$\Longrightarrow f \in \ker(ev_\alpha) = (m_\alpha)$$
$$\Longrightarrow m_\alpha \mid f \text{ in } \mathbb{Q}[x]$$

i.e. there exists $g(x) \in \mathbb{Q}[x]$ such that

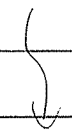
$$f(x) = m_\alpha(x)\, g(x).$$

Since $\deg(f) = 2$ this implies that

$$\begin{aligned} \deg(m_\alpha) &\leq \deg(m_\alpha) + \deg(g) \\ &= \deg(m_\alpha g) \\ &= \deg(f) = 2. \end{aligned}$$

But I claim that $\deg(m_\alpha) = 2$. If not then we must have $r, s \in \mathbb{Q}$ such that

$$m_\alpha(x) = r + sx \in \mathbb{Q}[x]$$



Evaluating at $x = \alpha$ gives

$$r + s\alpha = 0$$
$$r + s(1+\sqrt{3})/2 = 0$$
$$s(1+\sqrt{3}) = -2r$$
$$1+\sqrt{3} = -2r/s$$
$$\sqrt{3} = -2r/s - 1 \in \mathbb{Q}.$$

Contradiction. Hence $\deg(m_\alpha) = 2$ and we conclude that

$$m_\alpha(x) = x^2 - x - \frac{1}{2} \in \mathbb{Q}[x].$$

This the minpoly of α / $\mathbb{Q}$.

So what? Now suppose for contradiction that there exists monic $g(x) \in \mathbb{Z}[x]$ such that

$$g(\alpha) = 0.$$

Since $g \in \ker(ev_\alpha) = (m_\alpha)$ we have

$$g(x) = m_\alpha(x)h(x)$$

for some $h \in \mathbb{Q}[x]$.

Now we will use the famous

★ Gauss' Lemma:

We say that $f(x) \in \mathbb{Z}[x]$ is primitive if the gcd of its coefficients is 1. Let $f, g \in \mathbb{Z}[x]$ with g primitive. Then

$$g \mid f \text{ in } \mathbb{Q}[x] \implies g \mid f \text{ in } \mathbb{Z}[x].$$

In fact, if $f(x) = g(x)h(x)$ with $h \in \mathbb{Q}[x]$, it follows that $h(x) \in \mathbb{Z}[x]$.

Proof: See HW 3. ///

Back to our proof. We assume for contradiction that $\exists$ monic $g(x) \in \mathbb{Z}[x]$ with $g(\alpha) = 0$. Then

$$g \in \ker(ev_\alpha) = (m_\alpha)$$

means there exists $h(x) \in \mathbb{Q}[x]$ with

$$g(x) = m_\alpha(x) h(x).$$

But then

$$g(x) = \left(x^2 - x - \tfrac{1}{2}\right) h(x)$$
$$g(x) = \left(2x^2 - 2x - 1\right) \tfrac{1}{2} h(x).$$

Since $2x^2 - x - 1$ is primitive and $g(x) \in \mathbb{Z}[x]$, Gauss' Lemma says that

$$\tfrac{1}{2} h(x) \in \mathbb{Z}[x].$$

But then $g(x)$ has even leading coeff., contradicting the fact that it is monic.

Conclusion:

$\frac{1+\sqrt{3}}{2}$ is not integral over $\mathbb{Z}$.

You see that that was not terribly easy.

Why do we care?

We care because:

$\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ is a finitely generated $\mathbb{Z}$-module

$\mathbb{Z}\left[\frac{1+\sqrt{3}}{2}\right]$ is not finitely generated.

And we like finite things.

To get a feel for this we will first treat the case of

$$K \subseteq K[a]$$

where K is a field. In this case every polynomial is monic and things are easier.

Continuation of 2/20, 2/25, 2/27 lectures ...

Let $R \subseteq S$ be a ring extension

Recall: We say that $\alpha \in S$ is integral over R if $\exists$ monic $f(x) \in R[x]$ such that

$$f(\alpha) = 0.$$

We would like to prove the following. The set

$$\overline{R} := \{\alpha \in S : \alpha \text{ integral over } R\}$$

is a subring of S, called the integral closure of R in S.

To prove this is a bit tricky, so we first consider the case where

$$R = K$$

is a field (Körper).

Consider a ring extension $K \subseteq A$ of a field K.

Jargon: A is called a "K-algebra".

In particular, this makes A into a vector space over K. Under what conditions is A finitely generated (i.e. finite dimensional)?

Definition: We say that $\alpha \in A$ is algebraic over K if $\exists$ polynomial $\neq 0$ $f(x) \in K[x]$ such that

$$f(\alpha) = 0.$$

Otherwise we say that α is transcendental over K.

[Note: algebraic $\Longleftrightarrow$ integral over a field because every nonzero $f(x) \in K[x]$ is monic, because every nonzero $\lambda \in K$ is a unit.]

Now let $\alpha \in A \supseteq K$ be algebraic over K and consider the evaluation morphism

$$ev_\alpha : K[x] \longrightarrow A.$$

Recall that $K[\alpha] := \text{im}(ev_\alpha)$ is the smallest subring of A containing K and α. Since α is algebraic we have

$$\ker(ev_\alpha) \neq (0)$$

and since $K[x]$ is a PID we have

$$\ker(ev_\alpha) = (m_\alpha(x))$$

where $m_\alpha(x) \in K[x]$ is called the minimal polynomial of α over K.

Examples:

$$m_i(x) = x^2 + 1 \in \mathbb{R}[x]$$

$$m_{\frac{1+\sqrt{5}}{2}}(x) = x^2 - x - 1 \in \mathbb{Q}[x]$$

$$m_{\frac{1+\sqrt{3}}{2}}(x) = x^2 - x - \frac{1}{2} \in \mathbb{Q}[x].$$

Example:

If $A = Mat_n(K) \supseteq \{aI_n : a \in K\} = K$ then given a matrix $T \in A$ we call $m_T(x) \in K[x]$ the minimal polynomial of the matrix.

If $T = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \in Mat_2(K)$

over any field K then we have

$$T^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$

$$\Rightarrow \quad T^2 - I_2 = O_2$$

$$\Rightarrow \quad g(T) = O_2$$

where $g(x) = x^2 - 1$
$= (x-1)(x+1) \in K[x]$.

If $m_T(x) \in K[x]$ is the minpoly then

$$g(x) \in \ker(ev_T) = (m_T(x))$$

$$\Rightarrow \quad m_T(x) \mid g(x).$$

$\Rightarrow m_T(x) = x-1$ OR $x+1$ OR x^2-1.

But $m_T(T) = O_2$, whereas $T - I_2 \neq O_2$ and $T + I_2 \neq O_2$. Hence

$$m_T(x) = x^2 - 1 \in K[x].$$

Observe that the minpoly of a matrix need not be irreducible.

We may return to matrices but for now assume that $A \supseteq K$ is a domain. (Note: $\mathrm{Mat}_n(K)$ is not a domain).

Theorem: Let $A \supseteq K$ be a domain. Let $\alpha \in A$ be algebraic with minimal polynomial $m_\alpha(x) \in K[x]$. Then

- $m_\alpha(x)$ is irreducible over K.
- $K[\alpha]$ is a field.

Proof: Suppose $m_\alpha(x)$ factors as

$$m_\alpha(x) = f(x)\,g(x)$$

with $f(x), g(x) \in K[x]$ and

$0 < \deg(f), \deg(g) < \deg(m_\alpha)$. Evaluating at α gives

$$f(\alpha)\, g(\alpha) = m_\alpha(\alpha) = 0$$

$$\Rightarrow \quad f(\alpha) = 0 \quad \text{OR} \quad g(\alpha) = 0$$

because A is a domain. Without loss, say that $f(\alpha) = 0$, i.e., $f \in \ker(ev_\alpha) = (m_\alpha)$. This implies that

$$m_\alpha \mid f \Rightarrow \deg(m_\alpha) \leq \deg(f).$$

Contradiction. Hence m_α is irreducible.

Now since $m_\alpha(x) \in K[x]$ is irreducible and $K[x]$ is a PID we conclude that $(m_\alpha(x)) \leq K[x]$ is a maximal ideal. Hence

$$K[\alpha] \approx K[x] / (m_\alpha(x))$$

is a field.

Example: $\sqrt{2} \in \mathbb{R} \supseteq \mathbb{Q}$ is algebraic over $\mathbb{Q}$, thus

$$\mathbb{Q}[\sqrt{2}] = \{ f(\sqrt{2}) : f(x) \in \mathbb{Q}[x] \}$$
$$= \{ r + s\sqrt{2} : r, s \in \mathbb{Q} \}$$

is a field. Indeed, we have

$$\frac{1}{r+s\sqrt{2}} = \frac{1}{r+s\sqrt{2}} \left(\frac{r-s\sqrt{2}}{r-s\sqrt{2}} \right) = \frac{r - s\sqrt{2}}{r^2 - 2s^2}$$

$$= \left(\frac{r}{r^2-2s^2} \right) + \left(\frac{-s}{r^2-2s^2} \right) \sqrt{2} .$$

It is also true that $\mathbb{Q}[\sqrt[3]{2}]$ is a field, but this is not so obvious.

Q: How to compute the inverse

$$\frac{1}{r + s(\sqrt[3]{2}) + t(\sqrt[3]{2})} \in \mathbb{Q}[\sqrt[3]{2}] \quad ?$$

To solve this we need linear algebra.

///

Definition: Given a ring extension $A \supseteq K$ note that A is a vector space over K. We define

$$[A:K] := \dim_K(A).$$

★ **Theorem:** Let $\alpha \in A \supseteq K$. Then we have

$$[K[\alpha]:K] < \infty \iff \alpha \text{ is algebraic } / K,$$

in which case, $[K[\alpha]:K] = \deg(m_\alpha(x))$.

Proof: If α is transcendental then

$$K[\alpha] \approx K[x]/(0) = K[x].$$

By definition this is ∞-dimensional $/K$ with basis $1, x, x^2, x^3, \ldots$.

If α is algebraic let $m_\alpha(x) \in K[x]$ be the minimal polynomial and say that $\deg(m_\alpha(x)) = n \geq 1$. I claim that

$$1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$$

is a basis for $K[\alpha]$ over K.

First we show that $\{1, \alpha, \cdots, \alpha^{n-1}\}$ SPANS $K[\alpha]$. So consider any element $f(\alpha) \in K[\alpha]$. Divide $f(x)$ by $m_\alpha(x)$ to get

- $f(x) = q(x)\, m_\alpha(x) + r(x)$
- $r = 0$ OR $\deg(r) < \deg(m_\alpha)$.

Evaluate at α to get

$$\begin{aligned} f(\alpha) &= q(\alpha)\, m_\alpha(\alpha) + r(\alpha) \\ &= q(\alpha) \cdot 0 + r(\alpha) \\ &= r(\alpha) \\ &\in \operatorname{span}\{1, \alpha, \cdots, \alpha^{n-1}\}. \end{aligned}$$

Next we show $\{1, \alpha, \cdots, \alpha^{n-1}\}$ is INDEPENDENT. So suppose we have

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} = 0$$

for some $a_0, \cdots, a_{n-1} \in K$ and let $g(x) := a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in K[x]$. Note that $\deg(g) < n$. But since $g(\alpha) = 0$ we have

$$g(x) \in \ker(ev_\alpha) = (m_\alpha(x)).$$
$$\Rightarrow m_\alpha \mid g.$$

If $g \neq 0$ this implies that

$$n = \deg(m_\alpha) < \deg(g) < n$$

Contradiction. Hence $g(x) = 0$, which implies that

$$a_0 = a_1 = a_2 = \cdots = a_{n-1} = 0$$

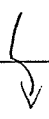
Slogan: "algebraic = finite"

Example: Let $\gamma \in \mathbb{C}$ be a root of the polynomial $x^3 - 2 \in \mathbb{Q}[x]$.

Claim: $x^3 - 2$ is irreducible / $\mathbb{Q}$.
If not then we have

$$x^3 - 2 = f(x)\, g(x)$$

where f or g has degree 1. WLOG suppose that $f(x) = x - a/b$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$.



But then evaluating at a/b gives

$$\left(\frac{a}{b}\right)^3 - 2 = f\left(\frac{a}{b}\right) g\left(\frac{a}{b}\right)$$

$$\frac{a^3}{b^3} - 2 = 0$$

$$a^3 = 2b^3$$

2 has mult $\equiv 0 \bmod 3$; 2 has mult. $\equiv 1 \bmod 3$

Contradiction. ///

Thus $m_\gamma(x) = x^3 - 2$ is irreducible, hence the minpoly of γ / $\mathbb{Q}$.

We conclude that

$$\mathbb{Q}(\gamma) = \{r + s\gamma + t\gamma^2 : r, s, t \in \mathbb{Q}\}$$

is a field. How can we compute the inverse

$$\frac{1}{r + s\gamma + t\gamma^2} = x + y\gamma + z\gamma^2 \quad ?$$

Expand

$$(r+s\gamma+t\gamma^2)(x+y\gamma+z\gamma^2) = 1+0\gamma+0\gamma^2$$

and equate coefficients to get

$$\begin{pmatrix} r & 2t & 2s \\ s & r & 2t \\ t & s & r \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

Solve using Gaussian elimination to get

$$(r+s\gamma+t\gamma^2)^{-1}$$

$$= \left(\frac{r^2-2st}{\Delta}\right) + \left(\frac{2t^2-rs}{\Delta}\right)\gamma + \left(\frac{s^2-rt}{\Delta}\right)\gamma^2$$

where

$$\Delta = r^3 + 2s^3 + 4t^3 - 6rst$$

is the determinant of the matrix. This is Galois theory.

Appendix For Fun: We can still make sense of "rationalizing the denominator" in $\mathbb{Q}(\gamma)$, but it's complicated.

Let $L \supseteq \mathbb{Q}$ be the splitting field of $x^3 - 2$ (the smallest field in which $x^3 - 2$ splits) and define the Galois group

$$\mathrm{Gal}(L, \mathbb{Q}) := \{\text{ring isomorphisms } \sigma : L \to L \text{ such that } \sigma(r) = r \ \forall r \in \mathbb{Q}\}.$$

One can show that $\mathrm{Gal}(L, \mathbb{Q})$ is isomorphic to the dihedral group of order 6.

Fact: Given any $\alpha \in L$ we have

$$\mathrm{Norm}_{L,\mathbb{Q}}(\alpha) := \prod_{\sigma \in \mathrm{Gal}} \sigma(\alpha) \in \mathbb{Q}.$$

Thus to "rationalize the denominator" we do this:

$$\frac{1}{\alpha} = \frac{1}{\alpha} \frac{\prod_{\sigma \neq 1} \sigma(\alpha)}{\prod_{\sigma \neq 1} \sigma(\alpha)} = \frac{\prod_{\sigma \neq 1} \sigma(\alpha)}{\mathrm{Norm}_{L,\mathbb{Q}}(\alpha)}.$$

Fun, right?

3/18/14

- Welcome Back!
- I have improved the Lecture Notes from 2/20, 2/25, 2/27. They will be on the web.
- HW 8 is due this Thurs
- NO CLASS NEXT TUES 3/25

Recall: Let $A \supseteq K$ be a ring extension of a field K (i.e. a "K-algebra").

For all $\alpha \in A$ we consider the evaluation morphism

$$ev_\alpha : K[x] \longrightarrow A$$
$$f(x) \longmapsto f(\alpha).$$

Since $K[x]$ is a PID we have

$$\ker(ev_\alpha) = (m_\alpha(x))$$

for some unique $m_\alpha(x) \in K[x]$ with leading coefficient 1. We call this the minimal polynomial of α over K.

If $m_\alpha(x) \neq 0$ we say α is algebraic over K.

It is interesting to consider minpolys of matrices $T \in Mat_n(K) \supseteq K$.
But right now we are interested in the case that $A \supseteq K$ is a domain.

☆ **Minimal Polynomial Theorem**
Let $A \supseteq K$ be a domain and suppose that $\alpha \in A$ is algebraic over K with $\deg(m_\alpha) = n$. Then

- $m_\alpha(x) \in K[x]$ is irreducible
- $K[\alpha] := im(ev_\alpha)$ is a field
- $[K[\alpha] : K] = \dim_K K[\alpha] = n$ with basis $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$.

Recall that

$$Frac(K[x]) = K(x)$$

$$:= \left\{ \frac{f(x)}{g(x)} : f, g \in K[x],\ g \neq 0 \right\}$$

By analogy we will define

$$K(\alpha) := \mathrm{Frac}(K[\alpha]).$$

Then we have

$$K(\alpha) = K[\alpha] \iff \alpha \text{ is algebraic } / K.$$

More generally we say that the ring extension $A \supseteq K$ is algebraic if

α is algebraic $/ K \quad \forall\ \alpha \in A$.

Theorem (Finite $\Rightarrow$ Algebraic):

Let $A \supseteq K$ be a ring extension of a field K. If $[A:K] = \dim_K(A) < \infty$ then A is algebraic over K.

Proof: Suppose $[A:K] = n < \infty$ and consider any element $\alpha \in A$. Since the set

$$1, \alpha, \alpha^2, \ldots, \alpha^n$$

is linearly dependent over K,

there exist $a_0, a_1, \dots, a_n \in K$ such that

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0.$$

Hence α is algebraic over K. ///

The converse is not true. For example, the set

$$\overline{\mathbb{Q}} := \{\alpha \in \mathbb{C} : \alpha \text{ algebraic over } \mathbb{Q}\}$$

is a ring extension (in fact a field extension) that is ∞-dim over $\mathbb{Q}$.

Q: Why is $\overline{\mathbb{Q}}$ a field?

Example: We know that $\sqrt{2}$ and $\sqrt[3]{2}$ are algebraic over $\mathbb{Q}$ with minpolys

$$f(x) = x^2 - 2 \quad \& \quad g(x) = x^3 - 2$$

To show that $\sqrt{2} + \sqrt[3]{2}$ is algebraic, we might look for $h(x) \in \mathbb{Q}[x]$ such that

$$h(\sqrt{2} + \sqrt[3]{2}) = 0.$$

Now we use a theorem.

Given $f(x) = \sum a_k x^k$ & $g(x) = \sum b_k x^k$ we define the <u>resultant</u>:

$$R(f,g) := \det \begin{pmatrix} a_0 & a_1 & \cdots & a_n & & \\ & a_0 & \cdots & a_{n-1} & a_n & \\ & & \ddots & & & \} m \\ & & & a_0 & \cdots & a_n \\ b_0 & b_1 & \cdots & b_m & & \\ & \ddots & & & \ddots & \\ & & b_0 & \cdots & & b_m \end{pmatrix} \} n$$

Then f, g have a common root in some field extension if and only if $R(f,g) = 0$.

Proof omitted ☺

So what? If $f(\sqrt{2}) = 0$ and $g(\sqrt[3]{2}) = 0$ we consider

$$f(x-y),\ g(y) \in \mathbb{Q}[y],$$

and define $h(x) := R(f(x-y), g(y)) \in \mathbb{Q}[x]$.

Then we will have $h(\sqrt{2}+\sqrt[3]{2}) = 0$ because the polynomials

$$f(\sqrt{2}+\sqrt[3]{2}-y),\ g(y) \in \mathbb{Q}[y]$$

have the common root $y = \sqrt[3]{2}$.
Let's do the computation: we have

$$\begin{aligned} f(x-y) &= (x-y)^2 - 2 \\ &= x^2 - 2xy + y^2 - 2 \\ &= (x^2-2) + (-2x)y + 1y^2. \end{aligned}$$

$$\begin{aligned} g(y) &= y^3 - 2 \\ &= -2 + 0y + 0y^2 + 1y^3. \end{aligned}$$

Hence.

$$h(x) = \det \begin{pmatrix} x^2-2 & -2x & 1 & 0 & 0 \\ 0 & x^2-2 & -2x & 1 & 0 \\ 0 & 0 & x^2-2 & -2x & 1 \\ -2 & 0 & 0 & 1 & 0 \\ 0 & -2 & 0 & 0 & 1 \end{pmatrix} \begin{matrix} \} 3 \\ \\ \\ \} 2 \\ \end{matrix}$$

$$= x^6 - 6x^4 - 4x^3 + 12x^2 - 24x - 4$$

Since $h(\sqrt{2}+\sqrt[3]{2}) = 0$ we conclude that $\sqrt{2}+\sqrt[3]{2}$ is algebraic over $\mathbb{Q}$. ///

That was not so easy. Here's an easy but nonconstructive proof.

Lemma (The Tower Law):

Given fields $E \supseteq L \supseteq K$ we have

$$[E:K] = [E:L] \cdot [L:K].$$

Proof: Let $E \supseteq L$ have basis

$$\alpha_1, \alpha_2, \cdots, \alpha_m$$

and let $L \supseteq K$ have basis

$$\beta_1, \beta_2, \cdots, \beta_n.$$

Then I claim that $E \supseteq K$ has basis

$$\{\alpha_i \beta_j : 1 \leq i \leq m, \ 1 \leq j \leq n\}.$$

- SPAN: Given

$$a = a_1 \alpha_1 + \cdots + a_m \alpha_m \in E$$

with $a_1, \cdots, a_m \in L$, we have

$$a_i = b_{i1}\beta_1 + \cdots + b_{in}\beta_n$$

for some $b_{ij} \in K$. Hence

$$a = \sum_i \left(\sum_j b_{ij}\beta_j \right) \alpha_i$$

$$= \sum_{i,j} b_{ij}\alpha_i\beta_j$$

- INDEPENDENT: Consider any elements c_{ij} such that

$$\sum_{i,j} c_{ij}\alpha_i\beta_j = 0.$$

Then $0 = \sum_i \left(\sum_j c_{ij}\beta_j \right) \alpha_i$ and since α_i are independent over L we have

$$\sum_j c_{ij}\beta_j = 0$$

for all i. Then since the β_j are independent over K we have

$$c_{ij} = 0.$$

for all i, j.

Now given a ring extension $A \supseteq K$ of a field K, we define the algebraic closure of K in A:

$$\overline{K} := \{\alpha \in A : \alpha \text{ is algebraic over } K\}.$$

Theorem: $\overline{K}$ is a field.

Proof: Consider any $\alpha, \beta \in \overline{K}$ with $\beta \neq 0$. We want to show that $\alpha - \beta, \alpha\beta^{-1} \in \overline{K}$. Well, we certainly have

$$\alpha - \beta, \alpha\beta^{-1} \in K(\alpha, \beta) := K(\alpha)(\beta)$$

Since α is algebraic over K we have

$$[K(\alpha) : K] < \infty.$$

Then since β is algebraic over K (hence also over $K(\alpha)$) we have

$$[K(\alpha)(\beta) : K(\alpha)] < \infty.$$

The Tower Law implies ↓

$$[K(\alpha,\beta):K] = [K(\alpha)(\beta):K]$$
$$= [K(\alpha)(\beta):K(\alpha)] \cdot [K(\alpha):K]$$
$$< \infty.$$

Then since $K(\alpha,\beta)$ is finite over K we conclude that every element of $K(\alpha,\beta)$ (including $\alpha-\beta$ and $\alpha\beta^{-1}$) is algebraic over K.

Hence $\alpha-\beta, \alpha\beta^{-1} \in \overline{K}$ and we conclude that $\overline{K}$ is a field

Here we used the key ideas

- Finite over Finite = Finite
- Finite $\Rightarrow$ Algebraic

Later we will try to mimic this proof over <u>rings</u>.

3/20/14

HW 3 due now.
NO CLASS NEXT TUES Mar 25.

HW 3 Discussion:

On this HW you worked through a family of results called "Gauss' Lemma".

The key fact is the following:

Let R be a PID so gcd's are defined. We say $f(x) \in R[x]$ is primitive if the gcd of its coefficients is 1. Then

$f, g \in R[x]$ primitive $\Rightarrow f \cdot g$ primitive

A useful Corollary says:

Let $K = \mathrm{Frac}(R)$. Suppose we have

$$f(x) = g(x)h(x)$$

with $f, g \in R[x]$, g primitive, $h \in K[x]$

Then actually $h(x) \in R[x]$.

We used this previously to show that

$\alpha = (1+\sqrt{3})/2$ is NOT integral / $\mathbb{Z}$

Proof: We showed that the minimal polynomial of α / $\mathbb{Q}$ is

$$m_\alpha(x) = 2x^2 - 2x - 1 \in \mathbb{Q}[x]$$

Now assume for contradiction that there exists monic $f(x) \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.

Since f is in the kernel of

$$ev_\alpha : \mathbb{Q}[x] \longrightarrow \mathbb{R},$$

i.e., $f(x) \in (m_\alpha(x))$, there exists $h(x) \in \mathbb{Q}[x]$ such that

$$f(x) = (2x^2 - 2x - 1)h(x).$$

Since $2x^2 - 2x - 1$ is primitive / $\mathbb{Z}$ Gauss' Lemma says that $h(x) \in \mathbb{Z}[x]$. This contradicts the fact that $f(x)$ is monic / $\mathbb{Z}$. ///

Gauss' Motivation was number theoretic.
He wanted to solve "Diophantine equations":

Given $f(x) \in \mathbb{Z}[x]$ find all $a \in \mathbb{Z}$ such that

$$f(a) = 0$$

[or maybe $f(a) \equiv 0 \mod p$]

Example: Solve $x^n + y^n - z^n = 0$ ☺

He found that passing to $\mathbb{Q}[x]$ was helpful

$$\mathbb{Z}[x] \rightsquigarrow \mathbb{Q}[x]$$
$$(\text{PID})$$

$\mathbb{Z}[x]$ is not a PID. For example,

$$(2, x) := \{ 2f(x) + xg(x) : f, g \in \mathbb{Z}[x] \}$$
$$= \{ \textstyle\sum a_k x^k \in \mathbb{Z}[x] : 2 \mid a_0 \}$$

is a non-principal ideal.

However we can use Gauss' Lemma to show

$\mathbb{Z}[x]$ is a UFD.

You showed on HW 3 that

R PID $\Longrightarrow$ $R[x]$ UFD.

It is not much harder to show that

$\boxed{R \text{ UFD} \Longrightarrow R[x] \text{ UFD}}$

[Some books humorously call this result "Gauss' Lemma"].

This result has an important corollary.

✡ **Theorem:** Let R be a UFD, for example $R = \mathbb{Z}$ or $R = K[x]$. Then

$R[x_1, x_2, \cdots, x_n]$ is a UFD.

Proof: Assume for induction that

$R[x_1, x_2, \cdots, x_{n-1}]$ is a UFD.

Then

$$R[x_1, \cdots, x_n] = (R[x_1, \cdots, x_{n-1}])[x_n]$$

is a UFD by Gauss' Lemma. ▨

Algebraic Geometry is concerned primarily with the rings

$$K[x_1, x_2, \cdots, x_n]$$

where K is an algebraically closed field. Our goal is to study such rings.

Let K be any field and consider a ring extension $A \supseteq K$ (i.e. a "K-algebra").

Then for any $a_1, a_2, \cdots, a_n \in A$ we have an evaluation morphism

$$ev_{a_1, \cdots, a_n} : K[x_1, \cdots, x_n] \longrightarrow A$$
$$f(x_1, \cdots, x_n) \longmapsto f(a_1, \cdots, a_n)$$

Let $K[a_1, a_2, \cdots, a_n] := \operatorname{im}(ev_{a_1, \cdots, a_n})$.

If $\ker(ev_{\alpha_1,\dots,\alpha_n}) = (0)$ we say that $\alpha_1, \alpha_2, \dots, \alpha_n$ are ALGEBRAICALLY INDEPENDENT over K. In this case we have

$$K[\alpha_1, \dots, \alpha_n] = \operatorname{im}(ev_{\alpha_1,\dots,\alpha_n})$$

$$\approx K[x_1, \dots, x_n]/(0)$$

$$= K[x_1, \dots, x_n].$$

If $\ker(ev_{\alpha_1,\dots,\alpha_n}) \neq (0)$ then there exists $f(x_1, \dots, x_n) \not\equiv 0$ such that

$$f(\alpha_1, \dots, \alpha_n) = 0$$

(an "algebraic relation" among the α_i)

and we say they are ALGEBRAICALLY DEPENDENT. (Generalization of linear algebra.) However, since $K[x_1, \dots, x_n]$ is not a PID, there is no analogue of the

"minimal polynomial"

Definition: We say that $A \supseteq K$ is "finitely generated as a K-algebra" if $\exists\, \alpha_1, \alpha_2, \ldots, \alpha_n \in A$ such that

$$A = K[\alpha_1, \ldots, \alpha_n] \quad \left(= \operatorname{im}(ev_{\alpha_1, \ldots, \alpha_n}) \right)$$

i.e., every $\alpha \in A$ can be expressed as a polynomial $\alpha = f(\alpha_1, \ldots, \alpha_n)$ over K.

In this case we have

$$A \cong K[x_1, \ldots, x_n] / \ker(ev_{\alpha_1, \ldots, \alpha_n}).$$

✡ Important Observation:

Every f.g. K-algebra has the form

$$A \cong K[x_1, \ldots, x_n] / I$$

for some ideal $I \leq K[x_1, \ldots, x_n]$.

✡ Important Question:

When do $I, J \leq K[x_1, \ldots, x_n]$ determine isomorphic K-algebras?

★ Important WARNING:

The notions of "K-algebra" and "K-module" (i.e. "K-vectorspace") are distinct. In particular, if $A \supseteq K$ is a K-algebra then

A is f.d. as a K-module "linear" $\Longrightarrow$ A is f.g. as a K-algebra. "polynomial"

But not the other way around. However we do have a partial converse.

Theorem: If $A \supseteq K$ is finitely generated as a K-algebra, say $A = K[a_1, \ldots, a_n]$, and if each generator a_i is algebraic / K, then $[A:K] = \dim_K(A) < \infty$.

Proof: Since a_1 is algebraic / K we know from Minimal Polynomial Theorem that

$K[a_1] = K(a_1)$ is a field

and $[K(\alpha_1) : K] = \deg(m_{\alpha_1}(x)) < \infty$.

Then since α_2 is algebraic over K (and hence over $K(\alpha_1)$) we have

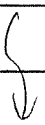
$$\begin{aligned} K[\alpha_1, \alpha_2] &= K[\alpha_1][\alpha_2] \\ &= K(\alpha_1)[\alpha_2] \\ &= K(\alpha_1)(\alpha_2) \\ &= K(\alpha_1, \alpha_2) \text{ is a field} \end{aligned}$$

and $$\begin{aligned} [K(\alpha_1, \alpha_2) : K] &= [K(\alpha_1)(\alpha_2) : K] \\ &= [K(\alpha_1)(\alpha_2) : K(\alpha_1)][K(\alpha_1) : K] \\ &= \deg(m_{\alpha_2}(x) \in K(\alpha_1)[x]) \cdot \deg(m_{\alpha_1}(x) \in K[x]) \\ &< \infty. \end{aligned}$$

By induction we conclude that

$$\begin{aligned} A &= K[\alpha_1, \dots, \alpha_n] \\ &= K(\alpha_1, \dots, \alpha_n) \text{ is a field} \end{aligned}$$

and $[A : K] < \infty$. //



Summary: Let $A \supseteq K$ be a K-algebra and consider the following conditions

(1) A is f.g. as a K-algebra.
(2) A is an algebraic extension of K.
(3) A is a Field.

We just proved that

$$(1) \ \& \ (2) \implies (3).$$

Q: Does $(2) \ \& \ (3) \implies (1)$?

A: NO. (Sorry)

However, it is true that

$$(1) \ \& \ (3) \implies (2)$$

"Weak Nullstellensatz"

while this seems innocuous (and boring!), it is the main technical lemma of Algebraic Geometry and the hardest thing we will prove in MTH 662. (After that, things will be downhill.)

3/27/14

No HW4 yet.

Recall: Let K be a field. We say that a K-algebra $A \supseteq K$ is finitely generated if $\exists\ a_1, a_2, \dots, a_n \in A$ such that the evaluation morphism

$$ev_{a_1,\dots,a_n} : K[x_1,\dots,x_n] \longrightarrow A$$
$$f(x_1,\dots,x_n) \longmapsto f(a_1,\dots,a_n)$$

is surjective. That is, we have

$$A = \operatorname{im}(ev_{a_1,\dots,a_n}) =: K[a_1, a_2, \dots, a_n].$$

If we let

$$I := \ker(ev_{a_1,\dots,a_n}) = \{ f \in K[x_1,\dots,x_n] : f(a_1,a_2,\dots,a_n) = 0 \}$$

then

$$A = K[a_1,\dots,a_n] \cong K[x_1,\dots,x_n] / I.$$

Thus to understand finitely generated K-algebras, we must understand ideals of the polynomial ring.

$$I \leq K[x_1, \dots, x_n]$$

UFD

This is our goal. ///

Let $A \supseteq K$ be a K-algebra and recall the following 3 properties:

(1) A is finitely generated as a K-algebra
(2) A is algebraic over K
(3) A is a field.

Last time we proved that

$$(1) \ \& \ (2) \implies (3).$$

The statement (2) & (3) $\implies$ (1) is FALSE.
Consider the algebraic closure of $\mathbb{Q}$ in $\mathbb{R}$ (or $\mathbb{C}$)

$$\overline{\mathbb{Q}} = \{ \alpha \in \mathbb{R} : \alpha \text{ algebraic } / \mathbb{Q} \}.$$

This is a field that is algebraic over $\mathbb{Q}$, but it is not finitely generated.

However, it is true that

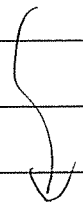
(1) & (3) $\Rightarrow$ (2).

That is, if $A \supseteq K$ is f.g. as a K-algebra and if A is a field, then A is algebraic over K.

This is called "Zariski's Lemma" and we will prove it soon.

But first,

"WHY would anyone care?"



Back to Philosophy:

We can think of $K[x_1, \ldots, x_n]$ as the ring of "polynomial functions" $K^n \to K$. For each $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ we define

$$f : K^n \longrightarrow K$$
$$(a_1, \ldots, a_n) \longmapsto f(a_1, \ldots, a_n).$$

Then for any set of points $S \subseteq K^n$ we consider the functions that vanish on S,

$$I(S) := \{ f \in K[x_1, \ldots, x_n] : f(\underline{a}) = 0 \ \forall \underline{a} \in K^n \}.$$

Note that $I(S)$ is an <u>ideal</u>.

<u>Proof</u>: Suppose that $f, g \in I(S)$ and $h \in K[\underline{x}]$. Then for all $\underline{a} \in S$ we have

$$\begin{aligned}(f - gh)(\underline{a}) &= f(\underline{a}) - g(\underline{a})h(\underline{a}) \\ &= 0 - 0 \cdot h(\underline{a}) \\ &= 0.\end{aligned}$$

Hence $f - gh \in I(S)$. ///

"I is for ideal."

Conversely, given any set of functions $T \subseteq K[\underline{x}]$ we consider their set of common zeroes,

$$V(T) := \{ \underline{a} \in K^n : f(\underline{a}) = 0 \ \forall \ f \in T \}.$$

☆ Definition:

A set $S \subseteq K^n$ is called algebraic (or an "affine variety") if

$$S = V(T) \text{ for some } T \subseteq K[\underline{x}].$$

"V is for variety." ///

Observation: The pair of maps

$$2^{K^n} \underset{V}{\overset{I}{\rightleftarrows}} 2^{K[\underline{x}]}$$

is an abstract Galois connection.

(See Lecture 1 of this course.)

For general reasons this implies that

(1) $V \circ I : 2^{K^n} \to 2^{K^n}$

$I \circ V : 2^{K[x]} \to 2^{K[x]}$

are closure operators. Recall that we say $cl : 2^U \to 2^U$ is a closure operator if for all $X, Y \subseteq U$ we have

- $X \subseteq cl(X)$
- $X \subseteq Y \implies cl(X) \subseteq cl(Y)$
- $cl(cl(X)) = cl(X)$.

We will say that $X \subseteq U$ is closed if

$$cl(X) = X.$$

(2) Given $S \subseteq K^n$ we have

S is closed $\iff$ $S = V(T)$ for some $T \subseteq K[x]$.

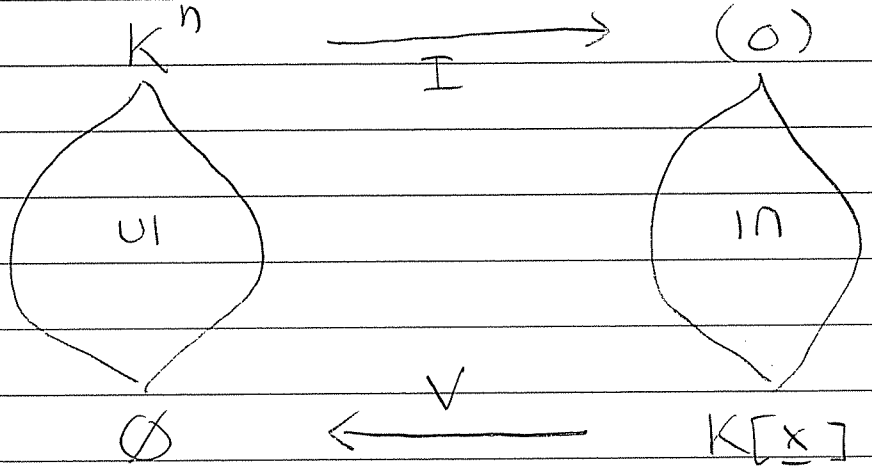
i.e. the closed subsets of K^n are the algebraic sets.

Given $T \subseteq F[\underline{x}]$ we have

T is closed $\iff$ $T = I(S)$ for some $S \subseteq K^n$.

i.e. the closed subsets are certain kinds of ideals. We don't yet have a name for these ideals.

(3) The maps I, V are order-reversing reciprocal isomorphisms between lattices of closed sets



This gives a "dictionary" between geometry and algebra.

All of that was abstract nonsense.
Now we look at special properties.

The properties

- $X \subseteq cl(X)$
- $X \subseteq Y \Rightarrow cl(X) \subseteq cl(Y)$
- $cl(cl(X)) = X$.

are not enough to define a topology.
In general, we also need

- $cl(X \cup Y) = cl(X) \cup cl(Y)$.

Luckily, in the case of varieties we do have this extra property.

Theorem: The union of two varieties in K^n is again a variety.

Proof: Suppose $S_1, S_2 \subseteq K^n$ are varieties, i.e., there exist ideals (in fact "closed" ideals) $T_1, T_2 \subseteq K[x]$ such that

$$S_1 = V(T_1) \quad \& \quad S_2 = V(T_2).$$

We will show that

$$S_1 \cup S_2 = V(T_1 \cap T_2),$$

and hence $S_1 \cup S_2$ is a variety.

First suppose that $\underline{\alpha} \in S_1 \cup S_2$, i.e., that $\underline{\alpha} \in V(T_1)$ OR $\underline{\alpha} \in V(T_2)$. Recall that V is order-reversing. Since

$$T_1 \cap T_2 \subseteq T_1$$
$$T_1 \cap T_2 \subseteq T_2$$

we have $V(T_1) \subseteq V(T_1 \cap T_2)$
$V(T_2) \subseteq V(T_1 \cap T_2)$.

Hence $\underline{\alpha} \in V(T_1 \cap T_2)$ and we conclude that

$$S_1 \cup S_2 \subseteq V(T_1 \cap T_2).$$

Conversely, suppose that $\underline{\alpha} \notin S_1 \cup S_2$. Since $\underline{\alpha} \notin S_1$, there exists $f \in T_1$ such that $f(\underline{\alpha}) \neq 0$, and since $\underline{\alpha} \notin S_2$, there exists $g \in T_2$ such that $g(\underline{\alpha}) \neq 0$.

Since K is a domain, we have

$$fg(\underline{a}) = f(\underline{a})g(\underline{a}) \neq 0.$$

Since $fg \in T_1 \cap T_2$ and $fg(\underline{a}) \neq 0$ we conclude that

$$\underline{a} \notin V(T_1 \cap T_2),$$

as desired. ///

Conclusion: The varieties in K^n are the closed sets of a topology, which we call the

"Zariski topology" on K^n.

Example: Describe the Zariski topology on K.

The closed sets have the form

$V(T)$ for an ideal $T \leq K[x]$.

Since $K[x]$ is a PID we have $T = (f(x))$ for some $f(x) \in K[x]$.

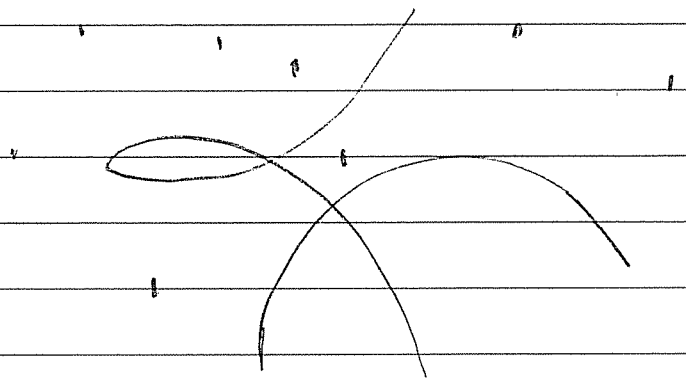
Then $V(T) = V(f(x))$ is just the set of zeroes of $f(x)$. If $\deg(f) = n$ then there are $\leq n$ of these.

Conclusion: The Zariski closed subsets of K are just the finite subsets.

(That's a rather strange topology...).

In K^n the finite sets are still closed, but there are other (higher dimensional) closed sets.

In K^2 a closed set looks like



4/1/14

No HW 4 yet.

Let K be a field and let $n \in \mathbb{N}$.

We will write

- $K[\underline{x}] := K[x_1, x_2, \ldots, x_n]$
- $\underline{\alpha} := (\alpha_1, \alpha_2, \ldots, \alpha_n) \in K^n$.

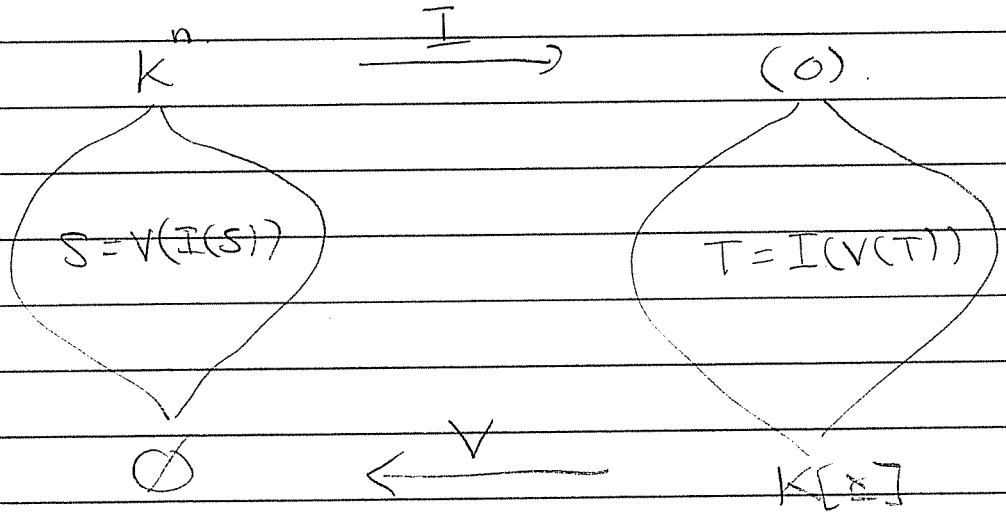
For all sets $S \subseteq K^n$ we define

$$I(S) := \{ f \in K[\underline{x}] : f(\underline{\alpha}) = 0 \ \forall \underline{\alpha} \in S \}.$$

and for all sets $T \subseteq K[\underline{x}]$ we define

$$V(T) := \{ \underline{\alpha} \in K^n : f(\underline{\alpha}) = 0 \ \forall f \in T \}.$$

This is an abstract Galois connection and we obtain an anti-isomorphism of lattices



Notation: If $S = V(I(S))$ then we say that $S \subseteq K^n$ is "Zariski closed", or an "affine variety".

If $J \subseteq K[\underline{x}]$ is any ideal then we have

$$V(I(V(J))) = V(J)$$

and so $S := V(J) \subseteq K^n$ is a closed set. We conclude that

closed subsets of K^n $\equiv$ zero sets of ideals of $K[\underline{x}]$

Suppose the ideal $J \subseteq K[\underline{x}]$ is finitely generated, i.e., suppose there exist

$$f_1, f_2, \ldots, f_k \in K[\underline{x}]$$

such that

$$J = (f_1, f_2, \ldots, f_k)$$
$$= \{ g_1 f_1 + \cdots + g_k f_k : g_1, \ldots, g_k \in K[\underline{x}] \}.$$

Then we have $\underline{a} \in V(J)$ if and only if $f_1(\underline{a}) = f_2(\underline{a}) = \cdots = f_k(\underline{a}) = 0$.

That is, $V(J)$ is the set of solutions to the finite system of polynomial equations:

$$\left.\begin{aligned} f_1(\underline{x}) &= 0 \\ f_2(\underline{x}) &= 0 \\ &\vdots \\ f_k(\underline{x}) &= 0 \end{aligned}\right\}$$

We would like to say that

Zariski closed set $\equiv$ solution of a system of polynomial equations,

But, do we know that every ideal of $K[\underline{x}]$ is finitely generated.

Put another way:

Is $K[\underline{x}]$ a Noetherian ring?

This is a famous result.

★ Hilbert's Basis Theorem (1890):

R Noetherian $\Longrightarrow$ R[x] Noetherian.

Proof: Let R be Noetherian, i.e., let R satisfy the two equivalent conditions

- every ideal of R is finitely generated.
- R has no infinite increasing chain of ideals.

We will show that every ideal of R[x] is finitely gen. So let $J \leq R[x]$ be an ideal and for all $n \in \mathbb{N}$ define the set

$$J_n := \{ a \in R : \exists\ f(x) = ax^n + \text{lower terms} \in J \}$$

$$= \{ \text{leading coefficients of polynomials } f(x) \in I \text{ of degree } n \} \cup \{0\}$$

Note that $J_n \leq R$ is an ideal since if $a, b \in J$ and $r \in R$ then $\exists$

$$f(x) = ax^n + \cdots, \quad g(x) = bx^n + \cdots \in J$$

Since J is an ideal, we have

$$f(x) - r g(x) = (a - rb)x^n + \cdots \in J,$$

hence $a - rb \in J_n$. ///

Since $f(x) \in J \Rightarrow xf(x) \in J$ we have.

$$J_1 \subseteq J_2 \subseteq J_3 \subseteq \cdots \subseteq R.$$

Since R is Noetherian, $\exists\, N$ such that

$$J_N = J_{N+1} = \cdots$$

Since R is Noetherian we also know that for all $n \in N$, the ideal J_n is finitely generated, say

$$J_n = (a_{n,1}, a_{n,2}, \cdots, a_{n,r_n}).$$

By definition, for each $n \in N$ and $1 \leq j \leq r_n$ there exists some polynomial

$$f_{n,j}(x) = a_{n,j}x^n + \cdots \in J.$$

I claim that the finite set

$$\{ f_{n,j}(x) : n \leq N, \ 1 \leq j \leq r_n \} \qquad (*)$$

generates J. Indeed, consider any $f(x) \in J$. Say that

$$f(x) = ax^m + \cdots .$$

If $m \geq N$ then $a \in J_m = J_N$ so that

$$a = \sum_i b_i a_{N,i} \quad \text{for some } b_i \in R$$

and then $f(x) - \sum_i b_i x^{m-N} f_{N,i}(x) \in J$ has degree $< m$.

If $m \leq N$ then $a \in J_m$ implies that

$$a = \sum_i b_i a_{m,i} \quad \text{for some } b_i \in R$$

and then $f(x) - \sum_i b_i f_{m,i}(x) \in J$ has degree $< m$.

We are done by induction on m.

Paul Gordan's reaction to Hilbert's proof:

"This is not mathematics. This is theology."
(He has a point)

In any case, if K is a field then by induction we conclude that

$K[x_1, \cdots, x_n]$ is Noetherian,

and hence that

Zariski closed subset of K^n $\equiv$ solutions of a finite system of equations $f(\underline{x}) = 0$ for $f(\underline{x}) \in K[\underline{x}]$

Notation: We say the ideal $J \subseteq K[\underline{x}]$ is closed if $J = I(V(J))$.

If $S \subseteq K^n$ is any set then we have

$$I(V(I(S)) = I(S)$$

and so $I(S)$ is a closed ideal.
We conclude that

$\downarrow$

closed ideal $\equiv$ functions that vanish
of $K[\underline{x}]$ on some set $S \subseteq K^n$.

Let's start with the easiest kind of set:

a point $\underline{a} \in K^n$.

Recall the evaluation map.

$$ev_{\underline{a}} : K[\underline{x}] \to K$$
$$f(\underline{x}) \mapsto f(\underline{a})$$

so that $I(\underline{a}) := I(\{\underline{a}\})$
$$= \{ f \in K[\underline{x}] : f(\underline{a}) = 0 \}$$
$$= \ker(ev_{\underline{a}}).$$

✡ Descartes' Factor Theorem (1637):

In the case of one variable $K[x]$ and $\alpha \in K$ we have

$$I(\alpha) = \ker(ev_\alpha)$$
$$= (x - \alpha)$$
$$= \{ (x-\alpha) g(x) : g(x) \in K[x] \}.$$

Proof: If $f(x) = (x-a)g(x)$ then clearly

$$f(a) = (a-a)g(a)$$
$$= 0 \cdot g(a) = 0.$$

Conversely, suppose that $f(a) = 0$ and divide by $(x-a)$ to get

- $f(x) = q(x)(x-a) + r(x)$
- $r(x) = 0$ or $\deg(r) < \deg(x-a) = 1$.
  (i.e. $r(x) = r \in K$ is a constant).

Evaluating at a gives

$$f(a) = q(a)(a-a) + r$$
$$0 = q(a) \cdot 0 + r$$
$$0 = r,$$

and hence $f \in (x-a)$. ///

What is the generalization of Descartes' Theorem in the ring

$$K[x_1, x_2, \ldots, x_n] \quad ?$$

Theorem: If $\underline{a} = (a_1, \ldots, a_n) \in K^n$ then the kernel of the evaluation

$$ev_{\underline{a}} : K[\underline{x}] \to K$$
$$f(\underline{x}) \mapsto f(\underline{a})$$

is given by

$$I(\underline{a}) = \ker(ev_{\underline{a}})$$
$$= (x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n)$$
$$= \left\{ g_1(x_1 - a_1) + \cdots + g_n(x_n - a_n) : g_i \in K[\underline{x}] \right\}$$

Proof: clearly

$$(x_1 - a_1, \ldots, x_n - a_n) \subseteq I(\underline{a}).$$

Conversely, consider any $f(\underline{x}) \in I(\underline{a})$. We can think of $f \in (K[x_2, \ldots, x_n])[x_1]$. Since $K[x_2, \ldots, x_n]$ is a domain and $x_1 - a_1$ is monic we can divide to get $g_1, r_1 \in K[x_2, \ldots, x_n]$ such that

- $f = g_1(x_1 - a_1) + r_1$
- $r_1 = 0$ or $\deg_{x_1}(r_1) < \deg_{x_1}(x_1 - a_1) = 1$

Thus we have $r_1 \in K[x_2, \dots, x_n] = (K[x_3, \dots, x_n])[x_2]$ and we can divide by $x_2 - a_2$ to get

- $r_1 = g_2(x_2 - a_2) + r_2$
- $r_2 \in K[x_3, \dots, x_n]$.

Continuing in this way we get

$$f = g_1(x_1 - a_1) + \cdots + g_n(x_n - a_n) + r$$

where $r \in K$ is constant. Evaluating at $\underline{a}$ gives

$$\begin{aligned} 0 &= f(\underline{a}) \\ &= g_1 \cdot 0 + \cdots + g_n \cdot 0 + r \\ &= r, \end{aligned}$$

hence $f \in (x_1 - a_1, \dots, x_n - a_n)$ as desired. ///

In fact the ideal $\ker(ev_{\underline{a}})$ is maximal because the evaluation $ev_{\underline{a}} : K[\underline{x}] \to K$ is surjective onto a field.

Q: Does every max. ideal of $K[\underline{x}]$ look like $I(\underline{a})$ for some $\underline{a} \in K^n$?

4/3/14

HW 4 due Thurs Apr 17

NO CLASS next Thurs Apr 10.

Final Exam Thurs May 1, 2-4:30 pm.

Last time we proved

☆ "Descartes' Theorem":

Let K be a field and consider a point $\underline{a} = (a_1, a_2, \ldots, a_n) \in K^n$. Then the evaluation morphism

$$ev_{\underline{a}} : K[\underline{x}] \longrightarrow K$$
$$f(\underline{x}) \longmapsto f(\underline{a})$$

has kernel

$$I(\underline{a}) = \{ f \in K[\underline{x}] : f(\underline{a}) = 0 \}$$

$$= (x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n). \quad ///$$

Proof: Given $f(\underline{a}) = 0$, divide by $x_1 - a_1$, Then divide the remainder by $x_2 - a_2$, etc. to get

$$f = g_1(x_1 - a_1) + \cdots + g_n(x_1 - a_n) + r$$

where $g_1 \in K[x_1, \cdots, x_n]$

$g_2 \in K[x_2, \cdots, x_n]$

$\vdots$

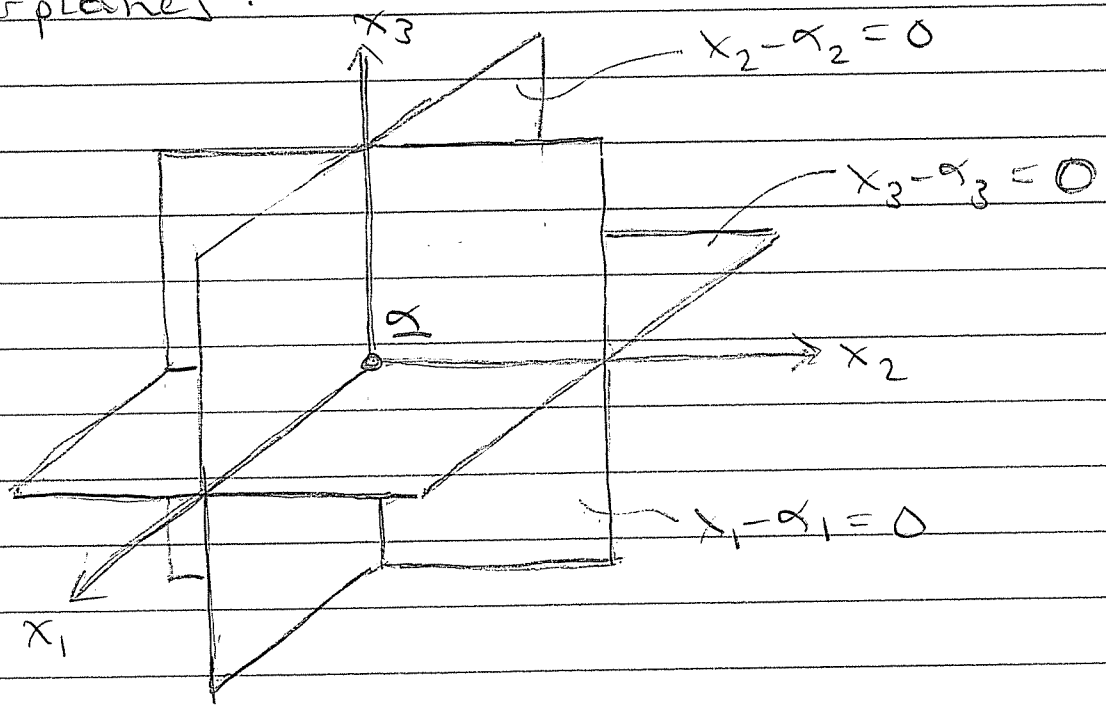
$g_n \in K[x_n]$

$r \in K$.

Evaluate at $\underline{x} = \underline{a}$ to get

$$0 = f(\underline{a}) = g_1(\underline{a}) \cdot 0 + \cdots + g_n(\underline{a}) \cdot 0 + r$$
$$0 = r.$$

Geometrically, this just says that $\underline{a} \in K^n$ is an intersection of coordinate hyperplanes:



In fact these ideals are maximal because evaluation at a is surjective onto the field K:

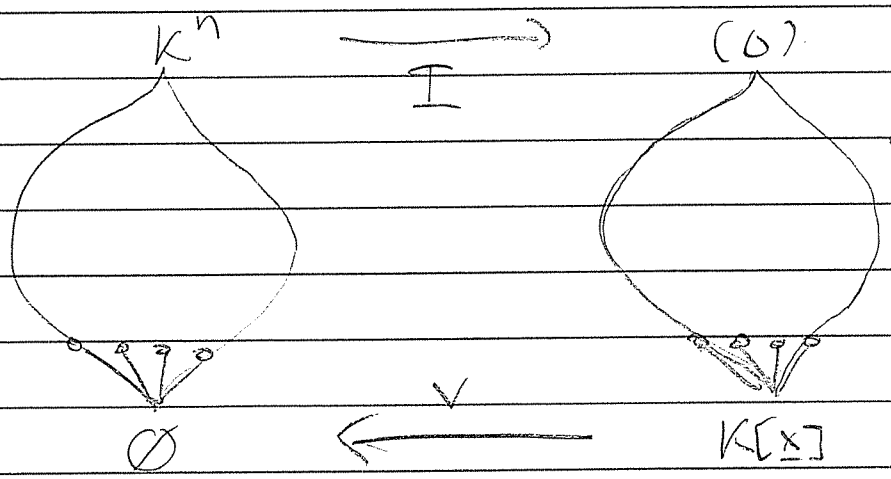
$$K = \mathrm{im}(\mathrm{ev}_a) \cong K[x]/\ker(\mathrm{ev}_a).$$

So I will prefer to write

$$\mathfrak{m}_a := \ker(\mathrm{ev}_a) = (x_1 - a_1, \ldots, x_n - a_n)$$

"The maximal ideal of the point $a \in K^n$" ///

Now recall the Galois connection:



We have a bijection

$$\{\text{min. closed sets}\} \underset{V}{\overset{I}{\rightleftarrows}} \{\text{max. closed ideals}\}$$

Since the minimal closed sets are just the points $\underline{a} \in K^n$, the maximal closed ideals are just the ideals $m_{\underline{a}} = I(\underline{a})$.

In fact the points $\underline{a} \in K^n$ are all of the minimimal sets (not necessarily closed).

Q: Are the ideals $m_{\underline{a}} < K[\underline{x}]$ all of the maximal ideals?

A: NO.

The ideal $(x^2+1) < \mathbb{R}[x]$ is maximal but it does not have the form

$$m_a(x) = x - a \in \mathbb{R}[x].$$

The maximal ideals of $\mathbb{R}[x]$ are in bijection not with $\mathbb{R}$ but with points in the closed upper half-plane

$$\overline{\mathbb{H}} := \{x+iy : x, y \in \mathbb{R},\ y \geq 0\} \subseteq \mathbb{C}$$

Proof: Since $\mathbb{R}[x]$ is a PID its maximal ideals are in bijection with irreducible polynomials. By the Fundamental Theorem of Algebra the irreducible polynomials have the form

- $x - \alpha$ for $\alpha \in \mathbb{R}$
- $(x-\alpha)(x-\overline{\alpha})$ for $\alpha \in \mathbb{H}$ ///

If we pass to the algebraic closure

$$\mathbb{C} = \overline{\mathbb{R}}$$

then we do get a bijection:

$$\begin{array}{ccc} \text{points of } \mathbb{C} & \longleftrightarrow & \text{max. ideals of } \mathbb{C}[x] \\ \alpha & & (x-\alpha) \end{array}$$

The same thing happens in higher dimensions

☆☆ Theorem (Hilbert's Nullstellensatz):

If K is an algebraically closed field, then every maximal ideal $\mathfrak{m} < K[x_1, \dots, x_n]$ has the form $\mathfrak{m} = \mathfrak{m}_{\underline{\alpha}}$ for some $\underline{\alpha} \in K^n$.

- The proof for $n=1$ is trivial.
- You will prove $n=2$ on HW4.
  It is not trivial.
- The proof for $n \geq 3$ is even less trivial but we will give it a try.

Try:

Let $m < K[x]$ be a maximal ideal and consider the field

$$L := K[x]/m.$$

Then consider the ring homomorphism

$$\varphi : K \longrightarrow L$$
$$\alpha \longmapsto \alpha + m$$

It is injective because $\alpha + m = \beta + m$ $\Longrightarrow \alpha - \beta \in m$. But since $m \neq K[x]$ we know that m contains no units (i.e. nonzero constants). Since $\alpha - \beta \in K$ we conclude that $\alpha = \beta$.

Thus we can view $\varphi : K \hookrightarrow L$ as a field extension. Furthermore, L is finitely generated (by $x_1+m, x_2+m, \cdots, x_n+m$) as a K-algebra.

It is a hard fact (called "Zariski's Lemma") that if $A \supseteq K$ is a K-algebra that is

- finitely generated,
- a field,

then A is algebraic over K. For now we will just assume this.

Hence L is algebraic over the subfield $\varphi(K) \approx K$. Since K was assumed algebraically closed this implies that

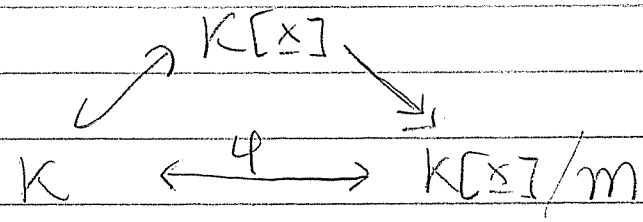
$$L = \varphi(K).$$

In other words, the map

$$\varphi : K \longrightarrow L = K[x]/m$$

is an isomorphism. (i.e. invertible).

Thus the following diagram commutes



Now for each $x_i + m \in K[x]/m$ define

$$\alpha_i := \varphi^{-1}(x_i + m) \in K.$$

So that

$$\begin{aligned}\varphi^{-1}(x_i - \alpha_i + m) &= \varphi^{-1}((x_i + m) - (\alpha_i + m)) \\ &= \varphi^{-1}(x_i + m) - \varphi^{-1}(\alpha_i + m) \\ &= \alpha_i - \alpha_i \\ &= 0\end{aligned}$$

and hence

$$\begin{aligned}x_i - \alpha_i + m &= \varphi(\varphi^{-1}(x_i - \alpha_i + m)) \\ &= \varphi(0) \\ &= m\end{aligned}$$

$$\Longrightarrow \quad x_i - \alpha_i \in m.$$

We conclude that

$$m_{\underline{a}} = (x_1 - a_1, \ldots, x_n - a_n) \leq m$$

and since we know already that $m_{\underline{a}} < K[\underline{x}]$ is maximal this implies $m = m_{\underline{a}}$.

Corollary: Let $J \leq K[\underline{x}]$ be an ideal. If K is algebraically closed then

$$J \neq K[\underline{x}] \iff V(J) \neq \emptyset.$$

Proof: If $J = K[\underline{x}]$ then clearly $V(J) = \emptyset$ (a nonzero constant function doesn't vanish anywhere).

Conversely, suppose that $J \neq K[\underline{x}]$. Then by Zorn's Lemma (HW4), J is contained in a maximal ideal

$$J < m < K[\underline{x}]$$

By the Nullstellensatz we have $m = m_{\underline{a}}$ for some point $\underline{a} \in K^n$.

But then

$$V(J) \supseteq V(m_{\underline{a}}) = \{\underline{a}\}$$

so J vanishes at the point $\underline{a} \in K^n$. ///

We can rephrase this:

The system of polynomial equations

$$\left.\begin{aligned} f_1(\underline{x}) &= 0 \\ f_2(\underline{x}) &= 0 \\ &\vdots \\ f_k(\underline{x}) &= 0 \end{aligned}\right\}$$

has a solution if and only if there do not exist polynomials $g_1(\underline{x}), \ldots, g_k(\underline{x})$ in $K[\underline{x}]$ such that

$$f_1 g_1 + \cdots + f_k g_k = 1 .$$

Q: There must be an algorithm (generalizing row-reduction) to decide this.

A: There is. It's called "Buchberger's Algorithm" (1976).