# Math 210 B with Ravi Vakil

Jared Marx-Kuo

Jan. 6th, 2020

## Contents

# 1/6/20

1. Logistics:
    - (a) Taught by Ravi Vakil, Office 383-Q
    - (b) Office hours TBA some time on Friday(?)
    - (c) CA is Lie Qian somewhere in the basement. Office hours TBA
    - (d) Make sure to check Canvas!
    - (e) Ravi wants to propose an alternate time of 9-10:20? On Tues/Thurs? Unsure, but he'll send out an email
    - (f) Grading is ALL HOMEWORK (no final)
    - (g) Homework is due on Wednesdays - no late homeworks allowed, but we can drop 1 homework over the quarter
2. Syllabus
    - (a) Advanced Field Theory
    - (b) Commutative Ring Theory (bulk of the class)
    - (c) Introduction to Representation theory (last few weeks)
3. Text References
    - (a) Jacobson Algebra 1 & 2
    - (b) Serge Lang's Algebra
    - (c) Dummit & Foote
4. The way we understand algebra is by thinking cleanly algebraically and geometrically
5. Field Theory
    - (a) We want to discuss ideas about fields that will generalize well enough to rings
    - (b) Why do we care about fields? Because Linear Algebra works over fields! And fields are built so that they work for linear algebra
    - (c) Before talking about fields, we need to define abelian groups and rings
    - (d) **Definition:** An Abelian group $G$ is a set with an operator $\cdot$, such that each element has an inverse, and it contains an identity element, $e$
    - (e) **Definition:** A ring (in this course) is an abelian group with two operations, $+$ and $\times$, and it contains an additive identity element, 0, and multiplicative identity, 1
    - (f) In this course, we'll assume that rings are commutative unless specified otherwise
    - (g) We WILL allow $1 = 0$ in our ring, in which case $R$ is the zero ring
    - (h) We also accept the axiom of choice to prove things like every non-zero ring has a maximal ideal - this is a common usage of axiom of choice
    - (i) **Definition:** A field is a ring where every element has an inverse under $\cdot$
    - (j) From a categorical perspective, we ask: what are maps of fields? $E \to F$ is inclusion
    - (k) This seems boring, but we can have many maps $E \to E$ which are not the identity. This implies a symmetry of the given field $E$
    - (l) Some examples of fields: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\overline{\mathbb{Q}}$, $\mathbb{F}_2$, $\mathbb{F}_q(t)$

(m) The characteristic is a map

$$\mathbb{Z} \to F \text{ s.t. } 1 \mapsto 1$$

Note the $\ker \phi$ will be a prime ideal BECAUSE $\mathrm{Im}(\phi)$ will be a subring of $F$ and hence an integral domain (any subring of a field cannot have zero divisors). By the first isomorphism theorem, this tells us that $\mathbb{Z}/\ker(\phi) \cong \mathrm{Im}(\phi)$ and so $\ker(\phi)$ must be prime.

(n) This tells us that either $\mathbb{F}_p \hookrightarrow F$ or $\mathbb{Z} \hookrightarrow F$ in which case $\mathbb{Q} \hookrightarrow F$

(o) Ravi wants us to think about prime ideals as things which quotient to give integral domains, and maximal ideals as things which quotient to give fields

(p) Category of fields, we have $E \hookrightarrow F$ and so

$$\begin{tikzcd} F \arrow[d] \\ E \end{tikzcd}$$

a field extension

(q) Examples of field extensions $\mathbb{C}/\mathbb{R}$, $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, $\mathbb{F}_4/\mathbb{F}_2$

(r) Consider the solution set $y^2 = x^3 - x$ over $\mathbb{C}$. Then $FF(y^2 = x^3 - x)$ (the fraction field of $y^2 = x^3 - x$) is a degree two extension of $\mathbb{C}(x)$ which is represented geometrically by a genus 1 surface (torus) covering a genus 0 surface (sphere). We'll come back to this later in the course

(s) What is the "size" of a field extension? Given a field extension, $E/F$, then $E$ is a vector space over $F$ (this will generalize later to modules)

(t) Then $\dim_F(E) =: \deg(E/F)$, which is a decent notion of size

(u) Another notion of size "size" would be $\mathbb{C}(t)/\mathbb{C}$, $\mathbb{C}(t_1, \dots, t_{10})/\mathbb{C}$ corresponding to 1 and 10 where the variables in the parenthesis are generators and we want to know how many generators we need. Other examples would be $\mathbb{C}/\mathbb{Q}$

(v) The above leads to the notion of "transcendence degree"

(w) **Definition:** The transcendence degree of a field extension is the largest number of algebraic independent elements of $E/F$

(x) Recall that algebraic dependence implies a polynomial relation

(y) Analogous to the linear case, we have a notion of a transcendence basis

(z) Aside: a Matroid is related to transcendence bases

6. More notes (counter was too big)

(a) Ex: The fraction field of $\mathbb{C}[x, y]/(y^2 - (x^3 - x))$ has transcendence degree 1 as an extension over $\mathbb{C}$

(b) Aside: is the above field, $E$, isomorphic to $\mathbb{C}(z)$ for some $z$? No, this is called Luroth's theorem and is an algebraic idea saying that there is no map from $S^2 \to T^2$.

(c) Is there an algebraic relation among

$$f = x^3 - y^2$$
$$g = x^4 + y^4 - xyh = x^{100} + x^{50} + y^{25}$$

apparently the answer is yes, and when we understand transcendence degree well, we'll know that whenever we have 3 functions in 2 variables, then these 3 functions are algebraically dependent

(d) More generally, for $n$ variables $\{x_1, \dots, x_n\}$ and $m$ polynomials, $\{f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)\}$. If $m \leq n$, there <u>may</u> be an algebraic relation among them. But if $m > n$, then there <u>is</u> an algebraic relation among them

(e) How to check the $m \leq n$ case? Consider $J\left(\frac{f_1,\dots,f_m}{x_1,\dots,x_n}\right) = \{\frac{\partial f_j}{\partial x_i}\}$. Then if there is an algebraic relation, then $J$ is not full rank!

**Proof:** If $g(f_1, \dots, f_m) = 0$, then

$$dg = \frac{\partial g}{x_1} dx_1 + \cdots + \frac{\partial g}{\partial x_n} dx_n = 0$$

when we expand the above, we'll get a linear dependence among the vectors $\partial f_i / \partial x_j$.

(f) Note that in characteristic 0, the above test is an if and only if! So this is a very useful test

# 1/8/20

1. Ravi says we'll do a quick review of Galois theory so we can extract the important ideas and use them for rings
2. We'll think about Fields with connections to integral domains and rings
3. The category of fields will be reminiscent of Galois Theory
4. Eventually, the category of rings will become affine schemes
5. Think of the examples: $\mathbb{Q}(\sqrt{2})$ vs. $\mathbb{Z}[\sqrt{2}]$
6. Note that transcendence degrees are not multiplicative like regular field extension degrees are. It's additive

$$\begin{tikzcd}
E \arrow[d, "tr.deg=e"] \\
G \arrow[d, "tr.deg=d"] \\
F
\end{tikzcd}$$

   and the transcendence degree of $E$ over $F$ is $d+e$.

7. Composition of fields

$$\begin{tikzcd}
& E_1E_2 & \\
E_1 \arrow[ur] & & E_2 \arrow[ul] \\
& F \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

   where $E_1E_2$ is the smallest field containing $E_1$ and $E_2$

8. Ravi points out that in order to define composite field, we need to talk about a larger ambient field, i.e. consider

$$\begin{tikzcd}
\mathbb{Q}[t]/(t^3-2) & & \mathbb{Q}(\sqrt[3]{2}) \\
& \mathbb{Q} \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

   What the is the composite of the top two fields? Unclear!

9. Really, our initial diagram should have been

$$\begin{tikzcd}
& D & \\
& E_1E_2 \arrow[u] & \\
E_1 \arrow[uur] \arrow[ur] & & E_2 \arrow[uul] \arrow[ul] \\
& F \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

   where we presume that $E_1, E_2 \subseteq D$ from the start

10. Algebraic elements

$$\begin{tikzcd}
\alpha \in E \arrow[d] & , & & F[\alpha] \arrow[d] & , & \text{s.t. } \phi(t) = \alpha \\
F & & F[t] \arrow[ur, "\phi"] \arrow[r] & E & &
\end{tikzcd}$$

then $\ker(\phi)$ is a prime ideal, so the kernel is 0 or a monic polynomial (because $F[t]$ is a Euclidean domain), the minimal polynomial

11. Claim: there exists a transcendental complex number. **Proof:** Algebraic numbers are countable, and $\mathbb{C}$ is uncountable, so there must exist a number which is not algebraic

12. For $\alpha$ algebraic, we have
$$F[\alpha] \cong F[t]/(m_\alpha(t))$$
this is a finite degree extension with degree equal to the degree of the polynomial

13. Converse: if $E/F$ is a finite degree extension, and $\alpha \in E$, then $\alpha$ is algebraic.
**Proof:** If $[E : F] = d$, then
$$1, \alpha, \alpha^2, \ldots, \alpha^d$$
must be linearly dependent, giving a non-zero polynomial $p(t)$ of degree at most $d$ such that $p(\alpha) = 0 \in E$

14. For
$$\begin{tikzcd} \alpha \in E \arrow[d] \\ F \end{tikzcd}$$
where $E$ is an arbitrary extension (not necessarily finite). Then $\alpha$ is algebraic if it is contained in a finite degree subextension.

15. Note that if $\alpha$, $\beta$ algebraic, then $\alpha \pm \beta \subseteq F(\alpha, \beta)$, which is a finite degree extension. So $\alpha \pm \beta$ is algebraic. Same for $\alpha\beta$.

16. Can define
$$\begin{tikzcd} E \arrow[dd] \arrow[dr] & \\ & E^{alg} \arrow[dl] \\ F & \end{tikzcd}$$
where $E^{alg}$ are elements which are algebraic over $F$, and they form a field. Furthermore, $E$ over $E^{alg}$ is a "purely transcendental" extension

17. Splitting Fields
    (a) For $f(t) \in F[t]$ irreducible, can make $F[t]/(f(t))$ field extension with degree equal to degree of the polynomial
    (b) **Definition:** A splitting field of $F$ (given $f(t) \in F[t]$) is
    $$\begin{tikzcd} E \arrow[d] \\ F \end{tikzcd}$$
    such that $f(t)$ factors into linear factors in $E[t]$. We require that $E$ is also minimal
    (c) The requirement that $E$ is minimal is fine because once we find a field where $f(t)$ splits, we can adjoin its roots to $F$ and just make that the minimal splitting field
    (d) Do splitting fields exist? Are they unique up to isomorphism? Are they unique up to unique isomorphism??? The answers are yes, yes, and no (in order)
    (e) We can at least add one root, by doing the following field extension
    $$\begin{tikzcd} F[u]/(g(u)) \arrow[d] \\ F \end{tikzcd}$$

and now looking at

$$g(t)/(t-u) \in (F[u]/(g(u)))[t]$$

So we can construct a splitting field by continuing to adjoint roots by looking at the irreducible multiplicands of $g(t)/(t-u)$, which is a polynomial

(f) How do we show that two splitting fields are isomorphic? Suppose we have another splitting field

$$\begin{tikzcd} Y \arrow[d] \\ F \end{tikzcd}$$

we make a subextension by mapping $u \in F[u]/(g(u))$ to one root of $g(t)$, all of which lie in $Y$. This gives a subextension $Y_1 = F(\alpha_1)$. Repeating this process for extensions above $F[u]/(g(u))$, we can repeat the process and make

(g) All of the choices we made were necessary and sufficient. And the degree of the extension is equal to $\deg g_k(u)$ with a number of choices equal to $\deg g_k(u)$, where $g_k$ is the reduced polynomial in the $k$th extension above $F$, with the first one being $F[u]/(g(u))[t]$

(h) This gives us the class $n!$ bound for the degree of the splitting field

(i) In addition, we learn that an isomorphism between splitting fields need not be unique, e.g. consider the automorphism $\mathbb{C} \to \mathbb{C}$ which sends $i \to -i$, but we could have chosen the identity automorpshim

(j) In general $|Aut(E/F)| \leq |E/F| = [E:F]$, but this works even when $E$ is not a splitting field. We prove this by building $E$ by adding generators one at a time

(k) **Definition:** If $|Aut(E/F) = |E/F|$, then $E$ is a Galois extension of $F$

(l) **Proposition:** Galois Extensions must be splitting fields (i.e. a normal extension).
**Proof:** This follows because as we build subextensions, we must have the correct number of choices each time, and we can take the product of the minimal polynomials we get at each step This part kind of flew over me

(m) Exercise: If $E/F$ is a splitting field, i.e. is a splitting field of some polynomial in $F[x]$, then any irreducible polynomial $g(t) \in F[t]$ which has one root in $E$ has all roots in $E$

(n) The above is useful, because it gives a characterization of a splitting field without a polynomial in mind

(o) Normality? I think he defined it in one of the above points

(p) **Definition:** If an irreducible polynomial, $f(t) \in F[t]$, has distinct roots in its splitting field, $E/F$, then the polynomial is called separable

(q) **Definition:** If $f(t) \in F[t]$ is any polynomial, not necessarily reducible, we say $f(t)$ is separable if every irreducible factor is separable

(r) **Definition:** If $\alpha \in E/F$ is algebraic then $\alpha$ is separable if $m_\alpha(t)$ is separable over $F[t]$

(s) **Definition:** Given $E/F$, and all $\alpha \in E$ are separable, we say $E/F$ is separable

(t) This raises the question, if we add to separable elements, $\alpha$ and $\beta$ of a field, then is the sum of those element separable? How about $\alpha/\beta$, $\alpha\beta$? If this is true, then we could get a field of separable elements

$$\begin{tikzcd} E \arrow[d] \\ E^{alg} \arrow[d] \\ E^{sep} \arrow[d] \\ F \end{tikzcd}$$

(u) We can also ask if $\alpha \in E$ is separable over $H$, is it separable over a subextension $F$? What about if $E/F$ separable and $F/H$ separable, then is $E/H$ separable?

18. Complex numbers example

    (a) Reasonable definition of $\mathbb{C}/\mathbb{R}$ is $\mathbb{C} := \mathbb{R}[x]/(x^2+1)$

    (b) Given $f \in \mathbb{C}$, we can write

    $$df = f_x dx$$

    but because of the way we formed $\mathbb{C}$, we need

    $$d(x^2+1) = 0 \implies 2xdx = 0 \implies xdx = 0 \implies dx = 0$$

    and so because everything can be written as $a + bx$, then $d(a+bx) = 0 + bdx = 0$ by the above. This seems like an unenlightening use of the derivative for field extensions

    (c) Let's consider another example: Let $k$ be a field of char $p$

    $$\begin{tikzcd} k(t) \arrow[d, "\deg\ p"] \\ k(t^p) = k(u) \end{tikzcd}$$

    where $k(t)$ becomes $k(u)[x]/(x^p - u)$. But then we have

    $$k(t)[x]/(x^p - u) = k(t)[x]/(x^p - t^p) = k(t)[x]/(x-t)^p$$

    We continue the computation

    $$df = f_x dx = d(x^p - u) = d(x^p) = px^{p-1}dx = 0$$

    because we're in characteristic $p$

19. Back to Galois theory

    (a) If $f(t) \in F[t]$, then $f(t)$ has a repeated root in its splitting field if and only if $f(t)$ and $D_t f(t) = f'(t)$ have a common factor

    (b) This result plays well with field extensions, so we can take $F$ to be the splitting field, i.e. $f(t) = (t-\alpha_1)\cdots(t-\alpha_n)$, so that by the product rule tells us

    $$f'(t) = \sum_{i=1}^{n} \prod_{j \neq i} (t - \alpha_j)$$

    and so there will be a nontrivial common factor iff $\alpha_i = \alpha_j$ for some $i \neq j$

    (c) Claim: If $f$ is irreducible and $f' \neq 0$, then $(f, f')$ are relatively prime

    (d) Claim: If $f(t) = g(t^p)$ and $p$ is the characteristic of the field, then $f'(t) = 0$

# 1/10/20

1. Today we discuss algebraic closures, differentials, and separability

    (a) Note that there is only one algebraic closure up to isomorphism so saying ”choose an algebraic closure” is misleading because there's only one

    (b) **Definition:** An algebraic closure of $k$ is a field extension such that all elements of $k[t]$ split completely in $\overline{k}[t]$ and no smaller subfield has this property

    (c) Note that this is a good definition compared to something like "the field of all algebraic elements over $k$" because then we need another ambient field to contain $\overline{k}$ to ask where these algebraic elements are coming from. E.g. it would be hard to define $\overline{\mathbb{Q}}$ without saying it's elements of $\mathbb{C}$ which satisfy polynomial relations over the rationals

    (d) With our definition though, we need to show existence though

    (e) Why is $\overline{k}$ algebraically closed itself?

(f) What are automorphisms of $\overline{\mathbb{Q}}/\mathbb{Q}$, or more generally $Gal(\overline{Q}/\mathbb{Q})$ when the extension is infinite?

(g) How do we show that algebraic closures are unique? We'll get something like

$$\begin{tikzcd}
 & & \overline{k} & & \\
\overline{k_1} \arrow[drr] \arrow[ddrr] & & & & \overline{k_2} \arrow[dll] \arrow[ddll] \\
 & & k(\alpha) \arrow[d] & & \\
 & & k & &
\end{tikzcd}$$

somehow we should be convinced that algebraic closures are isomorphic, though this is hard to show

2. Differentials

(a) We have

$$\begin{tikzcd}
A \\
B \arrow[u]
\end{tikzcd}$$

$A$ is a $B$-algebra, i.e. a ring which is also a $B$-module satisfying some multiplication rules like

$$b \cdot (a * c) = (b \cdot a) * c = a * (b \cdot c)$$

i.e. multiplication by $B$ commutes with whatever multiplication operation we have

(b) Differentials form some module over $C^\infty(\mathbb{R})$ generated by $\{df(x)\}$ for $f$ smooth and obeys the following relations: $d(fg) = dfg + fdg$ and $d(f + g) = df + dg$ and $d(\text{constant}) = 0$

(c) **Definition:** If $A$ is a $B$ algebra, then define the module of differentials of $A$ with respect to $B$ with generators $df$ for $f \in A$ and relations

i. $df + dg = d(f + g)$

ii. $d(fg) = fdg + gdf$

iii. $df = 0$ if $f \in B$

call this module $\Omega_{A/B}$

(d) Note that the last relation is equivalent to $d$ being $B$-linear, and we should also feel that $d(b) = 0$ is necessary because when $A = B$, then $df = 0$ for everything, but when $B \neq A$ this module becomes non-trivial

(e) Secretly, think of $\mathbb{C}^\infty(\mathbb{R})$ as an $\mathbb{R}$ algebra and $H(\mathbb{C})$ as a $\mathbb{C}$-alg

(f) Easy example is algebra of polynomials over $\mathbb{R}$ where

$$d(x^n) = nx^{n-1}dx$$

(g) If $A$ is generated over $B$ by $x, y \in A$, then $\Omega_{A/B}$ is generated by $dx$ and $dy$

(h) Can also consider functions on the circle $\{x^2 + y^2 - 1 = 0\} \subseteq \mathbb{R}^2$. Then functions on the circle are represented by $A = k[x, y]/(x^2 + y^2 - 1)$ and $B = k$. Then $\Omega_{A/B}$ is generated by $dx$ and $dy$ but with the following relation

$$d(x^2 + y^2 - 1) = 0 \iff xdx + ydy = 0$$

Ravi then points out that evaluating at different points gives us concrete relations between $dx$ and $dy$, so we should be thinking about this as a bundle of some sort.

(i) Another example: $y^2 = x^3 - x$ then the module is generated by $dx$ and $dy$ with the relation

$$2ydy + (1 - 3x^2)dx = 0$$

(j) In the above examples, the field wasn't specified (except for the fact that it's characteristic at least 3), so we have this differential relation if we worked with $C^\infty$ functions over $\mathbb{R}$ or Holomorphic functions over $\mathbb{C}$ or even finite fields

(k) Example: $y^2 = x^3 + x^2$ with the following relation

$$2ydy = (3x^2 + 2x)dx$$

note that this is a non-trivial relation when both of the functions are non-zero. This is a trivial relation when $2y = 0 = 3x^2 + 2x$, i.e. at $x = y = 0$. Thus, the tangency relation isn't defined at this point, which geometrically makes sense because the curve intersects itself at that point!

(l) This let's us redefine the notion of a smooth curve in $\mathbb{R}^2$ from "at least one of the partial derivatives does not vanish" to "there is a nontrivial relation between $dx$ and $dy$"

(m) Now we can make sense of tangent lines over finite fields

(n) Back to our original example of $\mathbb{C} = \mathbb{R}[x]/(x^2 + 1)$, then $\Omega_{\mathbb{C}/\mathbb{R}}$ is a complex vector space generated by the relation $2xdx = 0$ which means $dx = 0$

(o) Next example: $F = k[x]/(f(x))$ for $f(x)$ irreducible and so $\Omega_{F/k}$ is an $F$ vector space generated by $dx$ with the relation $d(f(x)) = f'(x)dx = 0$
From Galois theory, if $f'(x) = 0$, then $F/k$ is inseparable field extension and $dx \neq 0$. If $f'(x) \neq 0$, then it's a separable field extension and $dx = 0$. So our calculus relation tells us whether or not a field extension is separable, neat!

(p) **Theorem:** Consider

$$\begin{tikzcd} E \arrow[d] \\ F \end{tikzcd}$$

an algebraic extension. Then $x$ is separable over $F$ (i.e. the minimal polynomial for $x$) if and only if $dx = 0$. Moreover, $\Omega_{E/F} = 0$ implies $E/F$ is a separable extension

(q) This theorem is nice because it tells us that the sum, product, difference, and quotient of separable elements forms a separable field extension because $dx = 0$ and $dy = 0$ tell us that $dx+dy = 0$, $d(xy) = ydx+xdy = 0$, $d(x-y) = 0$ and $d(x/y) = (ydx - xdy)/y^2 = 0$. This all comes for free because separable means $dx = 0$.

(r) $E/F$ is purely inseparable if $E^{sep} \neq F$.

## 1/13/20

1. Reminder that there's no class Wednesday but the pset is still due
2. Office hours this week are being held by Lie (see website for time and place) and Ravi (probably on Friday)
3. IOU's: norms and traces
4. Last time: differentials

(a) Before, we had a transcendence basis where operations looked like linear algebra

(b) The notion of dimension of a transcendence basis played into geometry

(c) Reminder: Given a $B$-algebra, $A$, with $B \hookrightarrow A$ a ring morphism

(d) **Definition:** Given an $A$-module, $\Omega_{A/B}$, is the module of differentials of $A/B$, along with an operator $A \xrightarrow{d} \Omega_{A/B}$, where the map $d$ is **not** a map of $A$-modules, but is a map of $B$ modules, such that $a \mapsto da$ and the following rules hold

$$d(a + a') = da + da'$$
$$d(\alpha\beta) = (d\alpha)\beta + \alpha d(\beta)$$
$$db = 0 \qquad \forall b \in B$$

(e) We also require that $\Omega_{A/B}$ is universal with respect to these properties, i.e. a diagram

$$\begin{tikzcd}
\Omega_{A/B} \arrow[rd, "\exists!"] & \\
A \arrow[u] \arrow[r, "\text{B-module map}"] & M
\end{tikzcd}$$

Pretty sure that our $B$-module map $A \to M$ has to be a derivation, see here

`https://stacks.math.columbia.edu/tag/00RM`

(f) The reason we do this is that otherwise $\Omega_{A/B}$ = the zero module works.

(g) Another reason that $\Omega_{A/B}$ is useful is that we may choose to create this module in a different way, but it'll end up being the same

(h) Ex: If $A = B[x,y]/(f(x,y))$, then we can define $\Omega_{A/B} = \langle dx, dy\rangle/\{df = 0\}$ and check that this works

5. Commutative Ring Theory

(a) We're going to talk about algebra coming up in geometry

(b) Suppose we have an open set in a manifold, $M$, about a point $p$

(c) We can consider the ring of functions on $M$, $\mathcal{O}_M$, which follows because we can add and multiply them. It's also common to stipulate some condition on the functions, e.g. continuous, $C^\infty$, etc.

(d) The Evaluation map, $e_p$

$$\mathcal{O}_M \to \mathbb{R} \text{ s.t. } f \mapsto f(p)$$

then the kernel is a prime ideal, $\mathfrak{p}$

(e) Separately, we have a notion of "germs of functions near p." This object is a ring consisting of "shreds of functions which only remember what's going near $p$"

Formally, a germ consists of the collection of $(U, f)$ where $U \ni p$ is an open set and $f$ is a function on $U$, modded out by the equivalence relation $(U, f) \sim (U', f')$ if there exists $U'' \subseteq U, U'$ such that $f\Big|_{U''} = f'\Big|_{U''}$

(f) A germ really forms a ring under addition and multiplication, and we denote the germ of functions at $p$ by $\mathcal{O}_{M,p}$

(g) This comes with a natural homomorphism, evaluation at $p$, which is the only point which makes sense to evaluate it at (because manifolds are assumed to be Hausdorff)

$$\mathcal{O}_{M,p} \to \mathbb{R}, \qquad \text{s.t. } f \mapsto f(p)$$

(h) If $f \in \mathcal{O}_{M,p}$ and $f(p) \neq 0$, then we can choose a representative $(U, g)$ such that $g(p) \neq 0$. Note that $\{q \mid g(q) = 0\}$ is a closed set and we can define $U' = U \backslash \{q \mid g(q) = 0\}$. Now we can define $(U', \frac{1}{g})$, which provides an inverse.

Call this germ $\left(\frac{1}{g}\right)$, so that $f \times \frac{1}{g} = 1$

(i) Conclusion: if $f \notin \mathfrak{p} (= \ker(e_p))$ then $f$ is invertible in $\mathcal{O}_{M,p}$. This tells us that $\mathfrak{p}$ is maximal so that $\mathcal{O}_{M,p}$ forms a local ring $(\mathfrak{p} = m, \mathcal{O}_{M,p}, \mathbb{R})$, where the ordering is $(\text{maximal ideal}, \text{ring}, \text{quotient})$

(j) What we should really be thinking about are $\mathbb{R}$-analytic manifolds and tangent spaces. What is a tangent space? Could be the space of derivations at a point, but also:

(k) For $\Updownarrow$ an $R$-module, then $\Updownarrow/\Updownarrow^2$ is a $R/\Updownarrow = \mathbb{R}$ - module called the cotangent space. In fact it's a vector space with elements $f(x) - f(p)$. Then the tangent space is $(\Updownarrow/\Updownarrow^2)^*$.

(l) Another way to look at this is given maps

$$M \to M' \quad \text{ s.t. } \quad p \mapsto q \implies \mathcal{O}_{M',q} \to \mathcal{O}_{M,p}$$

which gives a map $\Updownarrow_q/\Updownarrow_q^2 \to \Updownarrow_p/\Updownarrow_p^2$

(m) Now we start: we're looking at $R = k[x_1, \ldots, x_n]/(\text{relations})$ where $k = \overline{k}$

(n) By the hilbert basis theorem, the relations we quotient out by in $R$ are finitely generated (because we're in a noetherian ring )

(o) From our set up

  i. Differential Geometers will think of the above straightforwardly

  ii. Complex geometers might think of analytic functions instead of polynomials as in the above

  iii. Number theorists will think about rings similar to $R$ and how we can compare them

  iv. An Algebra-Geometry correspondence

    A. $\overline{k}[x_1, \ldots, x_n]/(f_1, \ldots, f_r) \leftrightarrow$ a manifold cut out by nice equations

    B. $k[x_1, \ldots, x_n]/(f_1, \ldots, f_r) \leftrightarrow ??$

    C. $R \leftrightarrow Spec(R)$

  v. Consider a point $(a_1, \ldots, a_n) \in k^n$, then $I = (x_1 - a_1, \ldots, x_n - a_n)$ is a maximal ideal of $\overline{k}[x_1, \ldots, x_n]$ and we get an evaluation map

$$f \mapsto f(a_1, \ldots, a_n)$$

  yielding the quotient field $\overline{k}[x_1, \ldots, x_n]/I \cong \overline{k}$.

  vi. Similarly, $I = (f_1, \ldots, f_r)$ corresponds to the vanishing set $\{f_1 = f_2 = \cdots = f_r = 0\} = V(f_1, \ldots, f_r)$

  vii. Note that points of $V(f_1, \ldots, f_r)$ give maximal ideals of $k[x_1, \ldots, x_n]/(f_1, \ldots, f_r)$.

  viii. In particular, for $(a_1, \ldots, a_n) \in V(f_1, \ldots, f_r)$, then we get the following commutative diagram

$$\begin{tikzcd}
k[x_1, \ldots, x_n] \arrow[r, two heads] \arrow[d, two heads] & k[x_1, \ldots, x_n]/(x_1 - a_1, \ldots, x_n - a_n) \arrow[d] \\
k[x_1, \ldots, x_n]/(f_1, \ldots, f_r) \arrow[r, two heads] & k[x_1, \ldots, x_n]/(x_1 - a_1, \ldots, x_n - a_n)
\end{tikzcd}$$

  ix. **Theorem:** (Hilbert's weak Nullstellensatz) Ideals of the form $(x_1 - a_1, \ldots, x_n - a_n)$ where $(a_1, \ldots, a_n) \in V(f_1, \ldots, f_r)$ are the only maximal ideals of $\overline{k}[x_1, \ldots, x_n]/(f_1, \ldots, f_r)$

(p) **Lemma:** (Zariski's Lemma) Suppose that $E/F$ is a field extension and that $E$ is a finitely generated ring over $F$, then $E$ is a finite generated module over $F$

(q) We claim that Zariski's lemma implies weak hilbert:
**Proof:** Given $\mathfrak{m} \subseteq R = \overline{k}[x_1, \ldots, x_n]/I$ a maximal ideal, then $R/\mathfrak{m}$ is a field extension of $\overline{k}$, meaning that it is a finitely generated ring over $\overline{k}$ and thus a finite extension as a module over $\overline{k}$ (by Zariski's lemma), and so $R/\mathfrak{m} \cong \overline{k}$. This last step follows because we have that $R/\mathfrak{m}$ is a finite, and hence algebraic extension of our algebraically closed field, $\overline{k}$.

$$R \xrightarrow{/\mathfrak{m}} \overline{k}$$
$$x_1 \to a_1$$
$$\cdots$$
$$x_n \to a_n$$

## 1/17/20

1. No class Monday because of MLK day

2. Last Time

  (a) Finitely generated algebras over a field $k = \overline{k}$

  (b) Good examples: $k[x_1, \ldots, x_n]/(f_1, \ldots, f_r) = P/I$ where $P = k[x_1, \ldots, x_n]$ is a polynomial ring and $I = (f_1, \ldots, f_r)$ is the ideal of interest

  (c) Even if the ring is not algebrically closed, the maximal ideals look like $(x_1 - a_1, \ldots, x_n - a_n)$

  (d) Zariski's lemma: For $E/F$ a finitely generated algebra over $F$. The field extension $E$ is finitely generated vs. a finite extension over $F$, i.e. $E/F$ finite. These are **all** maximal ideals of $P_{\overline{k}}$ if $k \neq \overline{k}$. $I \subseteq P_k$ is maximal iff $P_k/I$ is a finite extension of $k$

  (e) Note that $E = k[t]$ is a finitely generated over $F = k$, but it is not a finite field extension. Of course $E = k[t]$ is not a field, so this isn't the best example of Zariski's lemma, BUT here's the idea: If we have a finite field extension, then the vector space structure and generators there gives you a finite generated algebra. The other direction of $E$ being a field and finitely generated algebra implies finite extension is murky on the intuition side and hence, where the "juice" of Zariski's lemma

3. More polynomial rings and algebras

   (a) $P/I$, then the ideals of $P/I$ correspond to ideals of $P$ containing $I$

   (b) Similarly, maximal ideals of $P/I$ correspond to maximal ideals of $P$ containing $I$

   (c) Algebra-geometry correspondence

$$P = \overline{k}[x_1, \dots, x_n] \overset{mSpec}{\leftrightarrow} F^n$$
$$m = (x_1 - a_1, \dots, x_n - a_n) \leftrightarrow (a_1, \dots, a_n)$$
$$P/(f_1, \dots, f_r) \leftrightarrow V(f_1, \dots, f_r) = \{\vec{a} \mid f_i(\vec{a}) = 0\}$$
$$B \to A \leftrightarrow mSpec(A) \to mSpec(B)$$
$$\overline{k}[y_1, \dots, y_n]/(g_1, \dots, g_r) \to \overline{k}[x_1, \dots, x_n]/(f_1, \dots, f_r) \leftrightarrow V(f_1, \dots, f_r) \to V(g_1, \dots, g_r)$$

   (d) What are the maximal ideals of

$$R = k[x, y]/(x^2 + y^2 - 25, (x-3)^2 + y^2 - 16, x^2 + (y-4)^2 - 9)$$

   probably $(x - 3, y - 4)$. This is the only maximal ideal, so the question is: is the above ring equal to $k[x, y]/(x - 3, y - 4)$? Yes, subtract the generators in the first ideal and you'll get the correct relations

   (e) Now look at $\mathbb{C}[x, y]/(y - x^2, y)$ and $\mathbb{C}[x, y]/(x, y)$. Then these two ideals have the same vanishing set, but whereas with the circle example, all three circles intersected transversally, the parabola and the line intersect tangentially, which is why $(y - x^2, y) \neq (x, y)$.

   (f) **Definition:** $mSpec(R)$ is the set of maximal ideals. Similarly $Spec(R)$ is the set of prime ideals

   (g) The name spectrum is similar to the notion of spectrum from linear algebra and functional analysis. Think of eigenspaces as prime ideals in a ring

   (h) $R$ acts on a field, $\overline{k}$. Then $R$ is a map to a field, this map corresponds to a maximal ideal $(x_1 - a_1, \dots, x_n - a_n)$

   (i) **Observe**: Given a map of finitely generated $\overline{k}$-algebra, i.e. $B \to A$, then we claim there is a direct reversing map $mSpec(A) \to mSpec(B)$

   (j) Ex:

$$B = k[t] \to k[x, y] = A \text{ s.t. } t \mapsto xy + xy^2$$

   then $(x, y) \mapsto (xy + xy^2)$

   (k) Ex:

$$B = k[x, y]/(y^2 - x^3) \to k[t] = A, \qquad x \mapsto t^2, \qquad y \to t^3$$

   pictorially, we're sending the line, $t$, to the curve $(t^2, t^3)$, but this latter curve is very not smooth at the point 0. This leads us to a proof that this map is not an isomorphism between our rings, $B$ and $A$. Informally, the tangent space should be something like $m/m^2$, which is one dimensional on the line representing $k[t]$ and two dimensional on the non-smooth point of the curve $y^2 - x^3$ representing $k[x, y]/(y^2 - x^3)$

   (l) Example of a ring map

$$B \to B/I, \qquad mSpec(B/I) \to mSpec(B)$$

   which we know from the start of class as $B/J$ maximal in $B/I$ gets mapped to $J$ maximal in $B$.

   (m) Example: Localization. Let $S$ be multiplicative set in $B$ (f.g. algebra over $\overline{k}$), then

$$B \to S^{-1}B \qquad \leftrightarrow \qquad mSpec(S^{-1}B) \to mSpec(B)$$

   assume that $S^{-1}B$ is a finitely generated algebra over $\overline{k}$. Then this map is injective, i.e.

$$mSpec(S^{-1}B) \hookrightarrow mSpec(B)$$

   this is because prime ideals of the localization correspond to prime ideals of $B$ which do not intersect $S$. The same holds for maximal ideals (which are prime), so we get the desired injection.

(n) Ex: $R = P/I$ (polynomial ring quotient by ideal), which is finitely generated over $\overline{k}$, then

$$S = \{f, f^2, \dots, \} \implies R_f \cong R[x]/(xf-1) \cong R[1/f]$$

What's the picture? This is the Rabinowicz trick. Think of $mSpec(R)$ for $\overline{k}[x,y]$ and then $mSpec(R_f)$ as $\overline{k}[x,y,z]/(z(y^2-x^3)-1)$. Then it's like looking at the graph $z = \frac{1}{y^2-x^3}$ away from the zero set of $y^2-x^3$. Similarly, we could think $k[x]_x = k[x,y]/(xy-1)$

The upshot is $mSpec(R_f) \hookrightarrow mSpec(R)$ where we map into ideals with vanishing sets in the complement of $V(f)$.

(o) Example (from before): $B = k[x,y]/(y^2-x^3) \to k[t] = A$ where $(x,y) \to (t^2,t^3)$. We want remove the point in the line corresponding to $A$, which then maps to the nonsmooth point in $B$. To remove the point in the line, localize by $t$, because $t$ vanishes at $t=0$. To remove the point in the curve, localize at $x$ because $x = 0 \implies y^2 - 0 = 0 \implies y = 0$. So we want to check

$$\left(k[x,y]/(y^2-x^3)\right)_x \cong k[t]_t$$

note that the map should be $(t-a_0) \mapsto (a_0^2, a_0^3)$, and in the other direction $(x_0,y_0) \in V(y^2-x^3)\backslash\{(0,0)\}$ maps to $y_0/x_0$.

To get the isomorphism between rings, we have $x \mapsto t^2$ and $y \mapsto t^3$ in one direction and in the other direction, we would wake $y/x$ which we should be thinking of as $(y=t^3)/(x=t^2) = t$

Note that if we localized at $\{y, y^2, \dots\}$, then we would do $x^2/y = t^4/t^3$ in the other direction, and in general we can do this when the powers of $t$ are relatively prime.

(p) Another example: $Spec(k[x]/(x^2))$ and $Spec(k)$

# 1/22/20

1. Tangent on Homework

   (a) We have $\Omega_{S/R}$ and the example $\Omega_{R[x]/R} = R[x]dx$

   (b) We do the example of $y^2 = x^3 - x$ over $k$, we take $S = k[x,y]/(y^2-x^3-x)$. Then $\Omega_{S/R} = (Sdx \oplus Sdy)/(2ydy - (3x^2+1)dx)$

   (c) If $2y \neq 0$, then $dy = \frac{3x^2+1}{2y}dy$, and vice versa when $3x^2+1$

   (d) This gets lengthy, but Ravi tells me to compare generators in the thing that we think is $\Omega_{S/R}$, i.e. where we have $df_i = 0$ for all $i$, and the more general definition and show that they are equivalent

2. For $R$ a ring, consider $Spec(R) = \{\text{prime ideals of R}\}$ and $mSpec(R) = \{\text{maximal ideals of R}\}$

3. Given a ring map $R \to S$, then we have a set map $Spec(S) \to Spec(R)$

4. Example: $R = \mathbb{C}[x]$, prime ideals are $(x-a)$ and $(0)$

5. Example: $R = \mathbb{C}[x,y]$, prime ideals are $(x-a, y-b)$, $(0)$, and $(f(x,y))$ irreducible because we're in a UFD

6. Example: $R = \mathbb{C}[x,y,z]$, prime ideals are at least points, ideals generated by irreducibles, and $(0)$, but it also contains other things like $(x,y)$, which is a prime ideal generated by two irreducibles

7. Now let's consider $R = \mathbb{Z}$, then this is a UFD and the prime ideals are $(p)$ and $(0)$ and the maximal ideals are all $(p)$ for $p \neq 0$

8. We can ask silly things like when does $20 = 0$? This makes sense if we're thinking of points as prime ideals, so $20 = 0$ at a prime $p$, when $20 \in (p)$, and so $20 = 0$ when $p = 2$ or $p = 5$

   We can also talk about, what is the value of 20 at other primes? I.e. 20 at the prime ideal $(3)$ is equal to 2 mod 3

9. Example: $R = \mathbb{R}[x]$, the primes are $(x-a)$, $(x^2+ax+b)$ where $a^2-4b < 0$

## 1/27/20

1. We have the following correspondence between algebra and geometry
   (a) Ring $P/I$ where $P = k[x_1, \ldots, x_n]$ corresponds to mSpec of $P/I$, a set
   (b) More generally, $R$ corresponds to Spec(R), a set
   (c) $P$, our polynomial ring, corresponds to mSpec $= k^n$
   (d) Maps of rings corresponds to maps of sets in the opposite direction
   (e) Finally, $f \in R$ corresponds to $f([p]) = f \mod P$ such that $f([p]) = 0 \iff f \in P$ for $P$ prime

2. Example: $V(xy, xz) \in \overline{k}[x, y, z]$. Then this vanishing set contains the $x = 0$ plane and the line $z = y = 0$.

   However, the prime ideal in Spec corresponding to this vanishing set is just $(x)$, which has a different vanishing set

3. Ravi is hinting at the idea of irreducible algebraic sets and the Zariski topology

4. Motivation, we have a bunch of equations in $\mathbb{C}[x, y, z]$, what do the solutions look like?

5. Hope: Given $f_1, \ldots, f_r$ in $\overline{k}[x_1, \ldots, x_n]$, then there are finitely many prime ideals, $\{p_i\}$ such that $\vec{a} \in V(f_1, \ldots, f_r)$ iff $\vec{a} \in V(p_i)$ for some $i$.

6. **Definition:** a Subset of (m)Spec(R) is closed in the Zariski topology iff it is cut out by some equations, i.e. $V(I)$ for some $I \subseteq R = k[x_1, \ldots, x_n]$

7. The Zariski topology will be defined with open sets being complements of the closed sets above

8. It's easy to verify that this collection of open/closed sets satisfy the axioms for a topology

9. **Definition:** A topological space is connected if $X = U_1 \sqcup U_2$ where $U_1$, $U_2$ open, then $U_1 = X$ or $U_2 = X$

10. **Definition:** A topological space is irreducible if $X = Z_1 \cup Z_2$ for $Z_1$, $Z_2$ closed then $X = Z_1$ or $X = Z_2$

11. Thinking about closures: consider the ideal $p = (0)$, what is its closure? Its the collection of all prime ideals which contain it, so all ideals in the spec

    What about $(x - a, y - b) \in \mathbb{C}[x, y]$? The only containing ideal is $(x - a, y - b)$ because its maximal. How about $(y^2 - x^3)$? We have $(x, y)$ and $(y^2 - x^3)$

12. More generally, irreducible closed subsets correspond to prime ideals in the spectrum

13. Qu: Given an irreducible closed subset, how do we get a prime ideal containing it? One idea is to take the intersection of all maximal ideals relevant, i.e. all maximal ideals whose vanishing sets are contained in our irreducible subset

14. Looking at $R = \mathbb{C}[t]_{(t)}$, then the only ideals are $(0)$ and $\{(t^n)\}_{n \geq 1}$ so the spectrum is just $(0)$ and $(t)$ and the mSpec is just $(t)$. This shows that our zariski topology is just two points and also that this intersection of maximal ideals construction is not good because look at $(0)$.

15. Exercise: Given a map $R_1 \to R_2$, then we have an induced map $Spec(R_2) \to Spec(R_1)$. Show that this map is continuous under the Zariski topology

## 1/29/20

1. I ask Ravi about what happens when some of the elements in $k$ from problem 21 on the last set have inseparable minimal polynomials

2. We look at the example of
$$x^p - a = (x - a^{1/p})^p$$
   in char $p$. Then $F = \mathbb{F}_p(u)$ and $u = v^p$ and $K = \mathbb{F}_p(v)$, then we can look at $F[t]$ and $(t^p - u) \in mSpecF[t]$. Note that in $\overline{F}[t]$, we have $t^p - u = t^p - v^p = (t - v)^p$.

   This tells us that $K/F$ is completely inseparable. And also we have that for $p = (t - v)$ then $\pi^{-1}\pi(p) = (t - v)$. This is not surprising because there are no Galois conjugates of $v$

3. Last time

   (a) Zariski Topology

   (b) A point $[p] \in \mathit{Spec}(R)$ is closed if and only if $p$ is maximal

   (c) Each point then forms a closed set (points correspond to maximal ideals

   (d) For finitely generated algebras we can equivalently look at $\mathit{mSpec}(\overline{k}[x_1, \ldots, x_n]/I)$

   (e) Ex: consider $\mathbb{Z}$, then every prime ideal is maximal and corresponds to a point on $\mathbb{Z}$. Note that $(0)$ which is not maximal and in fact $\overline{(0)} = \mathit{Spec}(\mathbb{Z})$

   (f) **Definition:** $p$ is said to be a generic point of $\overline{p}$

   (g) For any point $p$, $\overline{p}$ is irreducible closed subset

   (h) Universal counterexample (discrete valuation rings):

   $$k[x]_{(x)}, \qquad \mathit{Spec}(\mathbb{Z}_{(2)}) = \{(2), (0)\}$$

   note that $(2)$ is closed, i.e. $\overline{(2)} = (2)$, but $\overline{(0)} = \{(2), (0)\}$

4. **Definition:** In $\mathit{mSpec}\,\overline{k}[x_1, \ldots, x_n]/I$ or $\mathit{Spec}\,\overline{k}[x_1, \ldots, x_n]/I$, an irreducible component of a topological space is a maximal irreducible closed subset

5. In $\mathit{mSpec}$ of our polynomial ring, there are finitely many irreducible components, but this need not be true in a general $\mathit{Spec}(R)$

6. Remark: Any topological space is a union of irreducible components

7. Ex: $\mathbb{R}^n$ is the union of all points

8. **Definition:** A topological space is Noetherian if any decreasing sequence of closed subsets eventually stabilizes,

   $$X \supset Z_1 \supseteq Z_2 \supseteq \ldots$$

   then $\exists n_0$ such that $Z_i = Z_{i+1}$ for all $i \geq n_0$

9. Note that this is equivalent but contravariant to the definition of a noetherian ring, which makes sense because inclusion is reversed under containment of ideals vs. containment of vanishing sets

10. **Theorem:** $\mathit{mSpec}\; k[x_1, \ldots, x_n]/I$ as well as $\mathit{Spec}(\cdot)$ is a Noetherian topolgoical space (Not $\mathit{Spec}(R)$ in general)

11. Claim: Any closed subset of a Noetherian topological space has finitely many irreducible components. Moreover, such a closed decomposes as $Z = Z_1 \cup \cdots \cup Z_n$ where each $Z_i$ is irreducible, there is no redundancy among the $\{Z_i\}$'s and this decomposition is unique.
    **Proof:** Find a decomposition, then $Z_1 \cup Z_2 \cup \cdots \cup Z_n = Y_1 \cup \cdots \cup Y_n$. Want to show that $Z_1 = Y_i$ for some $i$. Do this by noting

    $$Z_1 = Z \cap Z_1 = (\cup_i Y_i) \cap Z_1 = \cup_i (Y_i \cap Z_1)$$

    but because $Z_1$ and $Y_i$ irreducible and $Y_i \cap Z_1$ is closed for each $i$, then we have that $Y_i \cap Z_1 = Z_1 = Y_i$ for some $i$ and $Y_j \cap Z_1 = \emptyset$ for all $i \neq j$

12. **Theorem:** For $R$ a Noetherian ring, $\mathit{Spec}(R)$ is a Noetherian topological space. In addition $\mathit{mSpec}\; k[x_1, \ldots, x_n]/I$ is a Noetherian topological space

13. Morally, we note that all increasing chains of ideal correspond to all decreasing chains of closed subsets

14. We will see that closed subsets correspond to ideals and also this is inclusion reversing and strict

15. **Definition:** If $S \subset \mathit{Spec}(R)$ (or $\mathit{mSpec}(R)$), define the ideal of functions vanishing on $S$ to be

    $$I(S) = \{f \in R \mid f(p) = 0, \;\; \forall p \in S\} = \bigcap_{[p] \in S} p$$

16. Remark: $I(S)$ is radical, i.e. $f^n \in I(S) \implies f \in I(S)$, i.e.

$$\sqrt{I(S)}$$

this is because $f^n \in \cap_{P \in S} P$ and so $f^n \in P$ for each individually. But prime ideals are radical so $f \in P$.

17. Algebra-Geometry correspondence

| Alg | Geometry/Topology |
|---|---|
| $R$ | $Spec(R)$, $mSpec(R)$ |
| $I(S)$ radical | $S \subset Spec(R)$ |
| $I$ | $V(I)$ closed subset of $Spec(R)$ |
| Prime Ideals | Irreducible closed subsets |
| Maximal ideals | Closed points |

18. Soon: We'll talk about how $V(\cdot)$ and $I(\cdot)$ give inclusion reversing bijection between closed subsets and radical ideals

19. Note that from the homework, we have $\sqrt{J} = I(V(J))$. Also, by definition $I_1 \subset I_2$ means that $V(I_1) \supset V(I_2)$, as well as $S_1 \subset S_2$ means $I(S_1) \supset I(S_2)$, so we actually have this correspondence except for the following fact

$$V(I(S)) = \overline{S}$$

20. To prove this final fact, we first show that $\overline{S} \subset V(I(S))$. Clearly $S \subseteq V(I(S))$ but $V(\cdot)$ always gives a closed subset, so $\overline{S} \subseteq V(I(S))$.

    Now note that

$$V(I(\overline{S})) = \overline{S}$$

    and so

$$S \subseteq \overline{S} \implies V(I(S)) \subseteq V(I(\overline{S})) = \overline{S}$$

    proving both directions

21. (Trivial Consequence) If $I \subset R$, we say a prime $P \subset R$ with $P \supset I$ is minimal if it is minimal among those primes containing $I$

22. If $R$ is Noetherian, then any $I$ has finitely many minimal primes

23. Claim: Suppose $R$ is a Noetherian ring. Then an ideal is radical iff it is the intersection of finitely many prime ideals
    **Proof:** On the homework, we showed that $\sqrt{I} = \bigcap_{P \supset I} P$, but $\sqrt{I}$ will correspond to a closed subset with finitely many irreducible components, and each irreducible component gives a minimal prime. So in particular $\sqrt{I} = \bigcap_{P \text{ minimal}} P$

24. Ravi says that every $Spec(R)$ has only one generic point

# 1/31/20

1. We need to prove the Nullstellensatz (finally)

2. We also need to rigorously define a notion of dimension that we've been dancing around

3. This will lead us to talk about finite/algebraic extensions of rings

4. **Definition:** A homomorphism of rings $\phi : R \to S$ is an extension of rings if $S$ is a finitely generated $R$-module. This is an integral extension of rings if for every $s \in S$, $s$ is integral over $R$, i.s. satisfies a monic polynomial with coefficients in $R$.

$$p(x) \in R[x], \quad p(x) = \sum_{i=0}^{n} a_i x^i, \qquad \in R, \quad p(s) = \sum_i \phi(a_i) \cdot s^i = 0 \in S$$

5. **Exercise**: Show that the property of a ring map being integral is preserved by quotient and localization of $R$ and quotient of $S$ but not necessarily localization of $S$

6. Ex: consider a $R \to R/I$, then the map $x - r$ works. Now consider $\mathbb{Z} \to \mathbb{Z}$, which becomes $\mathbb{Z} \to (\mathbb{Z} - \{0\})^{-1}\mathbb{Z}$ which is $\mathbb{Z} \to \mathbb{Q}$, then most elements in $\mathbb{Q}$ are not integrable over $\mathbb{Z}$

7. **Lemma:** Given $\phi : R \to S$ map of rings, THEN $s \in S$ integral over $R$ if and only if $s$ is contained in a sub-algebra of $S$ that is a finitely generated $R$-module.
   **Proof:** If $s \in S$ is alg. over $R$, then it satisfies some $p(s) = 0$ where $x^n + rx^{n-1} + \cdots + r_0$, and so $\phi(R)[s] \subseteq S$ is a finitely generated $R$ module.

   For the other direction, suppose otherwise, i.e. $s \in T$, where $T$ is a finitely generated $R$-module in $S$, i.e. $R \to T \subset S$, say generated by $m_1, \dots, m_n$. Then

   $$sm_i = \sum_j \alpha_{ij} m_j, \qquad s \begin{pmatrix} m_1 \\ \dots \\ m_n \end{pmatrix} = \begin{pmatrix} \alpha_{11} & & \\ & \dots & \\ & & \alpha_{nn} \end{pmatrix} \begin{pmatrix} m_1 \\ \dots \\ m_n \end{pmatrix}$$

   From here, we would want to multiply by $M^{-1} = \frac{1}{\det(M)} M^{adj}$, where $M^{adj}$ is the transpose of the matrix of cofactors and always exists. The problem is that $(\det M)^{-1}$ may not exist. Nonetheless we can multiply by the adjugate and so

   $$(sI - M) \begin{pmatrix} m_1 \\ \dots \\ m_n \end{pmatrix} = 0$$

   $$(sI - M)^{adj}(sI - M) \begin{pmatrix} m_1 \\ \dots \\ m_n \end{pmatrix} = \det(sI - M) \begin{pmatrix} m_1 \\ \dots \\ m_n \end{pmatrix}$$

   Note that $\det(sI - M)$ is a monic polynomial in $s$ with coefficients in $R$. THIS is 0 in $S$ because we always have that $1 \in T$ (assuming that $S$ is a ring with 1 then we can choose $T$ to have it as well), and so if we set $m_1 = 1$, then we get the result.

8. **Corollary:** : finite implies integral (for extension, and hence maps)

9. Exercise: Composition of finite integral rings is finite and integral

10. **Theorem:** (lying over) Suppose: $\phi : R \to S$ is an integral extension, then $Spec(S) \to Spec(R)$ is surjective

11. Motivating example: Consider

    $$\begin{tikzcd} \mathbb{C}[x,y]/(y^2 - x^3 + x) \arrow[d, dash] \\ \mathbb{C}[x] \end{tikzcd}$$

    what if we replace $\mathbb{C}$ by $\mathbb{R}$, then the variety induced by the above is a double cover of the variety induced by the lower, i.e. the real line

12. Other Motivating example: Consider

    $$\begin{tikzcd} \mathbb{Z}[i] \arrow[d, dash] \\ \mathbb{Z} \end{tikzcd}$$

    Then the point is that if we mod out the top by some large prime like $10^6 + 3$, then we'll get a ring which has maximal ideals. So above every prime in $\mathbb{Z}$ we get some primes in $\mathbb{Z}[i]$ lying over

13. The "lying over" phrase is motivated because we imagine prime ideals in the larger ring as being mapped to prime ideals in the smaller ring

14. Ex: $S = k$ and $R \hookrightarrow S = k$ $R$ a subring. Then if $\phi : R \hookrightarrow S$ is an integral extension and we have $Spec(S) \to Spec(R)$ surjective, then $Spec(S)$ is a point so we must have that $Spec(R)$ is a point, i.e. its a field. How do we show this?

$$\begin{aligned} a \in R, \quad a \neq 0, \implies a^{-1} \in S \implies \exists p(x) \in \phi(R)[x] \ \text{ s.t. } \ a^{-n} + r_{n-1}a^{-n+1} + \cdots + r_0 = 0 \\ \implies 1 + r_{n-1}a + \cdots + r_0 a^n = 0 \implies a^{-1} = -(r_{n-1} + \cdots + r_0 a^{n-1}) \end{aligned}$$

15. **Proof:** (of lying over theorem) To prove the lying over theorem, Ravi wants to reduce to the field case by localizing

$$\begin{tikzcd} S \arrow[d, dash] & Spec(S) \arrow[d] \\ R & Spec(R) \end{tikzcd}$$

If we want to show surjectivity, then it suffices to show that we hit $m \in Spec(R)$, with this we can consider the localization $R_m$, which will have unique maximal/prime ideal and so $R_m = R$ is a local ring. Let $p$ be any maximal ideal of $S_{(m)} = S$. Consider the following diagram

$$\begin{tikzcd} S \arrow[r] & S/p \\ R \arrow[u, hook] & R/p \cap R \end{tikzcd}$$

$S/p$ is a field and we claim that $R/p \cap R \to S/p$ is an integral extension. To see this, just take the integral relation for some $s \in S$ over $r$ and then pass it to the quotient side. But now we're in the field case and so we're done □

16. **Theorem:** (Going Up) Suppose $\phi : R \to S$ is an integral map of rings and

$$q_1 \subset q_2 \subset \cdots \subset q_m$$

are prime ideals of $R$. Suppose also that

$$p_1 \subset p_2 \subset \cdots \subset p_m \subset p_{m+1} \subset \cdots \subset p_n$$

are prime ideals of $S$ such that $q_i = \phi^{-1}(p_i)$. Then we can find $q_{m+1}, \ldots, q_n$ which are $\phi^{-1}(p_k)$ in some sense.

17. Note that it suffices to reduce to the $m = 1$ and $n = 2$ case.

## 2/3/20

1. A correspondence to review

| Fields | Rings |
|---|---|
| $\phi : R \to S$ extension | $\phi : R \to S$ morhpism |
| finite | finite |
| algebraic | integral |

note that finite implies algebraic/integral in the appropriate contexts

2. The notion of an algebraic extension gives rise to an algebraic closure, concurrently the notion of an integral extension gives rise to an integral closure

3. **Definition:** Suppose $R$ is an integral domain, then $R \hookrightarrow K(R)$, it's fraction field. We define the integral closure of $R$ to be those elements of $K(R)$ which are integral over $R$

4. More generally, given a field extension $F/K(R)$, we define the integral closure of $R$ inside of $F$

5. If $R$ is its integral closure (in $K(R)$) we say $R$ is integrally closed

6. Remark/Example: Integral closure in a field extension of $K(R)$ is integrally closed over $K(R)$

7. Ex: If $R = \mathbb{Z}$, what is the integral closure? i.e. the elements of $\mathbb{Q}$ which are integral over $\mathbb{Z}$. By the rational root theorem, we get $\mathbb{Z}$ itself

8. Ex: What about integral closure of $\overline{Q}$ over $\mathbb{Z}$? We call this the collection of algebraic integers, $\overline{Z}^{\overline{Q}}$

9. Ex: $R = \mathbb{C}[x]$? We take $F = K(\mathbb{C}[x,y]/(y^9 - x^{31} + x^7))$ this is a field extension of $\mathbb{C}(x)$ and so it makes sense to talk about the integral closure of $\mathbb{C}(x)$ over $F$

10. Ravi says that these objects are perfectoid spaces, but this seems like a high level perspective

11. **Claim**: If $R$ is a UFD, then $R$ is integrally closed.
**Proof:** The idea is the same as in the rational root theorem. We have

$$K(R) = \{\frac{a}{b} \mid a, b \in R \quad \text{and they have no common factors}\}$$

Any monic polynomial looks like

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 =$$

Plugging in $(a/b)$ and multiply by $b^n$ we get

$$a^n + a_{n-1}a^{n-1}b + \cdots + a_0 b^n = 0 \implies a^n = -b(a_{n-1}a^{n-1} + a_0 b^{n-1})$$

and so $b$ must be a unit, else $b \mid a^n$ a contradiction. Thus $\frac{a}{b} = \frac{c}{1} \in R \hookrightarrow K(R)$ for $c = ab^{-1}$. □

12. **Claim**: If $R$ is integrally closed and $D^{-1}R$ is any localization, where $0 \notin D$, then $D^{-1}R$ is also integrally closed.

**Proof:** $K(D^{-1}R) = K(R)$ from results about localization. Suppose that $x \in K(R)$ satisfies some monic polynomial over $D^{-1}R$, then

$$x^n + \frac{r_{n-1}}{d_{n-1}}x^{n-1} + \frac{r_{n-2}}{k_{n-2}}x^{n-2} + \cdots + \frac{r_0}{d_0} = 0$$

let $y = d_{n-1} \cdot d_{n-2} \cdots d_0 \cdot x$, then

$$y^n + r'_{n-1}y^{n-1} + \cdots + r'_0 = 0$$

then $y \in R$ because its integrally closed, and so

$$x = \frac{y}{d_{n-1} \cdots d_0} \in D^{-1}R$$

finishing the proof. □

13. **Proposition:** Suppose $A$ is an integral domain. Then TFAE

    (a) $A$ is integrally closed

    (b) $A_P$ is integrally closed for all $P$ prime

    (c) $A_M$ is integrally closed for all $M$ maximal

**Proof:** Note that from the previous claim, we have $(a) \implies (b)$, $(a) \implies (c)$, and also $(b) \implies (c)$ because every maximal ideal is prime. It then suffices to show that $(c) \implies (a)$:

Suppose $A$ is not integrally closed, there exists a monic

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

such that $p(r) = 0$ for some $r \in K(A) \backslash A$. Define $I \subset A$ as

$$I := \{b \ : \ rb \in A\}$$

this is clearly an ideal because its closed under addition and multiplication by arbitrary element of $A$. $I$ also contains 0. Note that $1 \notin I$ by construction, so $I \subseteq m$ for $m$ a maximal ideal

Now we want to show that $A_m$ is not integrally closed. We have that the coefficients $\{a_i\} \subset A \subset A_m$. HOWEVER, $r \notin A_m$ because

$$A_m = \{\frac{s}{q} \mid s \in A, \qquad q \in A \backslash m\}$$

and so $A_m$ is not integrally closed with the same polynomial. To verify this formally, we could probably do a proof by contradiction, i.e. suppose $\frac{a}{b} = \frac{c}{d}$ for $\frac{c}{d} \in A_m$, then

$$d \cdot \frac{a}{b} = \frac{c}{1} \implies d \in I \subset m$$

which can't happen □

14. Remark: In a Dedekind domain (soon!) all $A_m$'s are discrete valuation rings (soon!) which are UFDs and hence integrally closed

15. Examples of integrally closed domain without unique factorization :

$$\mathbb{C}[a,b,c,d]/(ad-bc) \qquad ad = bc, \qquad \frac{a}{c} = \frac{b}{d}$$

this looks like a good candidate for being not a UFD, but we have to verify that $\{a,b,c,d\}$ each are prime

16. Ex: $\mathbb{Z}[\sqrt{-\text{a large prime}}]$ will be integrally closed (most of the time?)

17. Dimension

    (a) Again returning to $\mathbb{C}[x,y]/(y^2 - (x^3 - x))$, Ravi says that this is a 1-dimensional complex manifold, but we want a ring oriented notion of dimension

    (b) **Definition:** (dimension of a vector space) The dimension of a vector space, $V$, is the length of the longest chain of strictly increasing subspaces of $B$, indexing start with 0, i.e.

    $$0 = V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_{n-1} \subsetneq V_n = V$$

    (c) Note that the above is a basis free way of defining the dimension of a vector space, and it is consistent with our definition for finite vector spaces because any two bases are of the same size

    (d) **Definition:** (dimension of a ring) The dimension of a ring is the supremum of the length of the chains of strictly decreasing prime ideals of $R$, where indexing starts with 0

    (e) The above is called the Krull dimension and has both algebraic and geometric meaning

    (f) Examples: $\mathbb{C}[x]$ then we have

    $$(x - a) \supset (0)$$

    is a chain of length 1

    (g) Remark: our definition of krull dimension is equivalent to if we took the supremum of the length of chains of increasing irreducible closed subsets of *Spec*$(R)$, via our correspondence between prime ideals and irreducible closed subsets

    (h) Ex: For $\mathbb{C}[x,y]$ we have

    $$(x - a, y - b) \supset (f(x,y)) \supset (0)$$

    for $f(x,y)$ an irreducible polynomial. Thus krull dimension is 2

    (i) Ex: For $\mathbb{C}[x,y,z]$, we're kind of stuck because we don't have a nice characterization of prime ideals in this ring

    (j) Ex: $\mathbb{Z}$, then $\dim(\mathbb{Z}) = 1$

    (k) Ravi says that we can call rings of dimension 1 a curve, and rings of dimension 2 a surface. Not sure how faithful this description is

    (l) Using this, we think of a spectrum which consists of a curve, disjoint union with a point. The former can be created *Spec*$(\mathbb{C}[x])$ and the latter as *Spec*$(\mathbb{F}_2)$. From the homework, we have that

    $$Spec(\mathbb{C}[x] \times \mathbb{F}_2) = Spec(\mathbb{C}[x]) \sqcup Spec(\mathbb{F}_2)$$

    and so we really have this spectrum as a "curve" and a "point" for the ring, $\mathbb{C}[x] \times \mathbb{F}_2$

(m) For prime ideal, $p \subset R$, we define the codimension (aka the "height") of $p$ is the supremum of the lengths of chains of strictly decreasing chains of prime ideals starting at $p$

(n) With this, the codimension of $0 \times \mathbb{F}_2$ in our previous example is 0. Similarly, we could take the generic point on $\mathbb{C}[x]$ and get codimension/height 0

(o) We want this notion of codimension to behave nicely, but Ravi draws a picture of a line intersecting a plane in $\mathbb{R}^3$ transversally to show that codimension doesn't behave as well we thought, i.e. it depends on which subvariety you choose in order to create a chain of prime ideals

(p) Final hope: the codimension of one prime ideal in an other should be independent of the chain

(q) Such rings where the above holds are called "catenary" rings

(r) **Theorem:** finitely generated algebraic extensions over fields are catenary

(s) **Theorem:** (proved sometime this week) Suppose $R$ is an integral domain, finitely generated over a field. Then $K(R)$ is a finitely generated field extension of $k$ and

$$\dim R = tr\ \deg\left(K(R)/k\right)$$

(t) As an example: $\dim \mathbb{C}[x, y, z] = 3$, which was very hard to tell from before

(u) Remark: If $R$ is a UFD, then all codimension 1 prime ideals are principal.

**Proof:** Suppose $p \subset R$ is codimension 1, i.e. $0 \subseteq q \subseteq p$, then $q = 0$ or $q = p$. Take any $f \in p$. Factor it into irreducibles, $f = f_1 \cdots f_n$. Then by primeness $f_i \in p$ for some $i$, but then

$$0 \subsetneq (f_i) \subsetneq p$$

then $(f_i) \neq 0$ and $(f_i)$ is prime so $(f_i) = p$

(v) Note, this is not true in general, e.g. take $(x - a, y - b) \subseteq \mathbb{C}[x, y]$

## 2/5/20

1. Last time

   (a) We talked about finite/integral extensions, as well as morphisms, of a ring

   (b) We also defined krull dimension

2. Dimension:

   (a) We want krull dimension to be reasonable, so let's check that the topological dimension of a manifold over some field $k$, cut out by algebraic equations, matches the krull dimension

   (b) Immediate caveat: We would want our field to be algebraically closed, else we could note that the manifold $x^2+y^2+z^2 = 0$ is 0 dimensional topologically over $\mathbb{R}$, however the krull dimension of $\mathbb{R}[x, y, z]/(x^2+y^2+z^2)$ is 1

3. Extensions

   (a) Context is a map from a field to a ring, $k \to R$,

   (b) Question: What are finite extensions (i.e. the rings) of a field?

   (c) Given $k \to R$ finite extension, $R$ has many prime ideals and all are maximal
   **Proof:** We have that $R = k[x_1, \ldots, x_n]/I$. Any prime $p$ of $R$ gives $R/p$ an integral domain, which is finitely generated as a vector space over $k$. From past classes, we showed that this means that every element is invertible and hence we have a field.

   To see finitely many prime ideals, this follows because $k[x_1, \ldots, x_n]/I$ is Noetherian and hence has finitely many minimal prime ideals □

   (d) Remark: We could replace "finite extension" with "integral extension" and we'll get that all prime ideals are maximal

(e) Claim: If $k \to R$ is an integral extension, then every prime ideal of $R$ is maximal.
**Proof:** If $P$ is prime and $x \neq 0$ in $R/p$. Because it's an integral extension, we would get

$$x^n + a_1x^{n-1} + \cdots + a_n = 0 \in R/p \implies x^{-1} = \frac{-1}{a_n}(a_1x^{n-1} + \cdots + a_1)$$

showing that it's a field. □

(f) The above tells us that $\dim R = 0$

(g) **Proposition:** If $R \to S$ is an integral ring extension, then $\dim R = \dim S$

**Proof:** Pictorially, Ravi draws $Spec(S)$ as some curve lying over $Spec(R)$, which is represented as a line. Moreover, $Spec(S)$ looks like a multi-cover of $Spec(R)$. The crux of this proof is the going-up and going-down theorem

The idea is as follows

$$\begin{gathered} q_0 \supsetneq q_1 \supsetneq \cdots \supseteq q_m \\ p_0 \supsetneq p_1 \supsetneq \cdots \supseteq p_m \end{gathered}$$

and so if we have a chain of prime ideals in $Spec(R)$ then we can pull them back to a chain of primes in $S$. The only tricky part is to show that strict increasing is preserved.

To get around this, we look at

$$K(R/p) = R_p/pR_p$$

and consider maps

$$R \to R/p \to FF(R/p)$$

where $FF(R/p)$ means the fraction field. From this, we get that the fiber over the localization/quotient will give us a field as a quotient of $R$, and then the corresponding quotient of $S$ will be an integral extension. In the integral extension, we will have that every prime ideal is maximal, and this translates into strict inclusions

A little more formally: we have $p \subset R$, we do

$$\begin{tikzcd}
 & R \arrow[dl] \arrow[dr] & \\
R_p \arrow[dr] & & R/p \arrow[dl] \\
 & R_p/pR_p = K(R/p) = FF(R/p) &
\end{tikzcd}$$

The above diagram is to show that quotienting and localization commute. Given a map of Spec's you get a map of these as topological spaces. Ravi then claims that the fiber over $P \in Spec(R)$ is the same as the prime/maximal ideals of $R_p/pR_p$.

(h) **Theorem:** "dim = tr. deg." Suppose $R = k[x_1, \ldots, x_n]/p$ is an integral domain. Then

$$\dim R = \text{trdeg} K(R)$$

Before we prove, we have a few corollaries

(i) **Corollary:** $\dim k[x_1, \ldots, x_n] = n$

(j) **Corollary:** Nullstellensatz/ Zariski's lemma follows, i.e. if $R = k[x_1, \ldots, x_n]/M$ for $M$ a maximal ideal, then $R$ is a finite dimensional vector space over $k$
**Proof:** $Spec(R)$ will be a point because of the third isomorphism theorem. Then $\dim R = 0$ so $trdeg_k(R) = 0$ by our theorem, i.e. every element is algebraic over $k$. As such

$$\exists p_i \in k[x_1, \ldots, x_n] \text{ s.t. } p_i(x_i) = 0 \in R = k[x_1, \ldots, x_n]/M, \implies (p_1(x_1), \ldots, p_n(x_n)) \subseteq M$$

and so

$$k[x_1, \ldots, x_n]/\left(p_1(x_1), \ldots, p_n(x_n)\right) \twoheadrightarrow R$$

□

(k) Observation: "The dimension of such $R$ can be computed on any nonempty open set"

(l) The above agrees with our topological definition of dimension, and we want to claim that $\dim Spec(R) = \dim(U)$ for $U$ a topologically open set

(m) Consider $R = k[x]_{(x)}$. Then $Spec(R) = \{(0), (x)\}$ where $\overline{(0)} = Spec(R)$. This is bad because any open set containing $(0)$ will contain $(x)$ and so the topological dimension will disagree with the krull dimension, the latter of which is 1 because $(0) \subset (x)$. The reason this doesn't contradict our observation is that the set up is not the same because $k[x]_{(x)}$ is not finitely generated over a field

(n) For $R = k[x_1, \dots, x_n]/P$ as before, consider

$$S = R_f = k[x_1, \dots, x_n, y]/(p, yf - 1)$$

dimension of $R$ is the transcendence degree of the fraction field. But if we take the fraction field of $R_f$, then this is the same as the fraction field of $R$, and so the dimension of $R_f$ is the same as the dimension of $R$. This motivates us to think of the following open set $Z((f))^c$, i.e. the collection of prime ideals which do not contain $f$

(o) We want: Given any $I = (0)$ for $I = I(U^c)$, want an $f \neq 0$ that vanishes on $V(I)$, i.e. $f^N \in I$. Any element of $I$ that isn't 0 works, which shows that the open set of $Z((f))^c$, will give us the same dimension

(p) With this, we'll finally prove that transcendence degree equals the dimension of the ring

4. **Lemma:** (Noether Normalization Lemma): Suppose that $R$ is an integral domain, finitely generated as an algebra over $k$, i.e.

$$R = k[t_1, \dots, t_s]/P$$

for $P$ prime. If $tr\deg_k K(R) = n$, then we can find $x_1, \dots, x_n \in R$ which are algebraically independent such that $R/k[x_1, \dots, x_n]$ is an integral extension where $k[x_1, \dots, x_n] \hookrightarrow R$ (i.e. no kernel of this map!)

5. Note: Noether Normalization Lemma (NNL) implies that transcendence degree equals the dimension of the ring because an integral extension of a ring has the same dimension as the ring

6. Remark: This is like manifold theory, where if we know the dimension of a little bit of $\mathbb{R}^n$, then we know the dimension of a manifold

7. Before we prove the NNL, we need to show that $\dim k[x_1, \dots, x_n] = n$. The dimension is at least $n$ because of $(x_1) \subset (x_1, x_2) \subset \cdots \subset (x_1, x_2, \dots, x_n)$. To show the other bound, if we have

$$0 \subset p_1 \subset \cdots \subset p \subset k[x_1, \dots, x_n]$$

then Ravi says we can compute

$$tr\deg\left(k[x_1, \dots, x_n]/p\right) = n - 1$$

8. We now prove that $\dim = tr\deg$ by induction on $n = tr\deg_k K(R)$. For $n = 0$, this is trivial (why?). Assume for all "smaller $n$" Take $R$ with $tr\deg K(R) = n$. By NNL, $\dim R = \dim k[x_1, \dots, x_n]$, so

$$\dim k[x_1, \dots, x_n] \geq n$$

and we'll see that there there is no longer chain than $n$.

Suppose we have a chain of length greater than $n$:

$$0 \subsetneq p_1 \subsetneq \cdots \subsetneq p_m \subset k[x_1, \dots, x_n]$$

Then take any $f \neq 0$ in $p_1$ and factor

$$f = \prod_{j=1}^{\ell} f_j$$

some $f_j$, call it $g$, is in $p_1$, then

$$tr\deg K\left(k[x_1, \dots, x_n]/(g)\right) = n - 1$$

so the chain starting at $g$ must be length $\leq n - 1$, i.e.

$$0 \subsetneq (g) \subset p_1 \subsetneq \cdots \subsetneq p_m \subset k[x_1, \dots, x_n]$$

We certainly have $(g) \subseteq p_1$, but there may be equality. This gives us the bound in the other direction.

## 2/7/20

Ravi cancelled class

## 2/10/20

1. We're almost done with commutative ring theory
2. The plan
   (a) We'll discuss Noether normalization which will help us get a hold on dimension
   (b) We'll also discuss Discrete valuation rings (and hence Nakayama's lemma), Dedekin domains, both of which are dimension 1
   (c) We'll also discuss norm/trace, which is vital for the going-down theorem. This will be our overview of the dimension 0 case for rings
   (d) Later, we'll discuss representation theory
3. **Theorem:** If $R$ is an integral domain, finitely generated over a field, $k$, them $\dim R = tr \deg K(R)/k$
4. Remember that here we're thinking of $R = k[t_1, \ldots, t_n]/(p)$ for some $p$ a prime ideal
5. Noether Normalization lemma: Under some hypothesis; if $tr \deg K(R)/k = n$ then we can find $x_1, \ldots, x_n \in R$, algebraically independent such that $R/k[x_1, \ldots, x_n]$ is a finite extension.
   **Proof:** Write $R = k[y_1, \ldots, y_m]/p$. Note that $m \geq n$ where $n = tr \deg K(R)/k$, because the transcendence basis will be a subset of the image of $\{y_1, \ldots, y_m\}$ in the fraction field, $K(R)$. If $m = n$, then $p = 0$ (else we would have some set of relations in $p$, which would translate to fewer generators in the fraction field) and we win! So we choose to prove this by induction with the base case of $m = n$.

   Now if $m > n$, then the plan is to consider

$$\begin{tikzcd}
R = k[y_1, \ldots, y_m]/p \arrow[d, dash] \\
k[z_1, \ldots, z_{m-1}]/q \\
k[x_1, \ldots, x_n] \arrow[u, hook]
\end{tikzcd}$$

   i.e. find some $\{z_1, \ldots, z_n\}$ and a prime ideal $q$ and apply induction after we find this embedding.

   Now if $p \neq 0$, then there exists $f \in k[t_1, \ldots, t_m]$ such that $f \neq 0$ and

$$f(y_1, \ldots, y_n) = 0 \in k$$

   the idea is to take some random projection of $\{y_1, \ldots, y_{m-1}\}$ onto the "span" of $y_m$ and then subtract this projection off and get a new variable. Formally

$$z_1 := y_1 - y_m^{r_1}$$
$$z_2 := y_2 - y_m^{r_2}$$
$$z_{m-1} := y_{m-1} - y_m^{r_{m-1}}$$

   then

$$f(z_1 + y_m^{r_1}, z_2 + y_m^{r_2}, \ldots, z_{m-1} - y_m^{r_{m-1}}, y_m) = 0$$

   we want to make $r_1$ big, $r_2$ even bigger, and so on so that eventually we'll get some term $cy_m^{\text{huge}} + \ldots$ where $c \in k$ and for the other summands, we think of this as a polynomial in $y_m$ with coefficients in $k[z_1, \ldots, z_{m-1}]$. After dividing by $c$, we get a monic polynomial so that $y_m$ is integral over $k[z_1, \ldots, z_{m-1}]$. From here, induction applies. □
6. Note that finite implies integral

7. Rmk: Suppose $\ell/k$ is a field extension and $R$ is finitely genearted integral domain over $k$, and $R \otimes_k \ell$ is an integral domain, THEN $\dim(R) = \dim(R \otimes_k \ell)$, e.g. $k = \mathbb{Q}$ and $\ell = \mathbb{C}$ so that we'll get $\overline{Q}$

8. Goal: **Theorem:** "codimension = difference of dimensions for finitely generated algebras (which are also integral domains) over a field.

   (a) Translation: if $R$ is a finitely generated algebra over a field and we have that $P \subseteq Q$ prime ideals, then $\dim R/P = \dim R/Q +$ codimension of $(P \subseteq Q)$

   (b) Remark: If $X \subsetneq Y$ irreducible and $X$ is closed in $Y$, then $\dim X < \dim Y$.

   (c) **Proof:** (of theorem) New goal: If $\dim R/p - \dim R/q > 1$, then we can find an intermediate prime ideal $I$, with
   $$q \supsetneq I \supsetneq p, \quad \dim R/I = \dim R/p - 1$$
   Strategy for the new goal: we have the map
   $$\begin{tikzcd} R/q & \\ R/p \arrow[u] & \\ k[x_1, \dots, x_n] \arrow[u, hook, "\text{finite ext. by NNL}"] \arrow[r, dash, "\supset"] & q \cap k[x_1, \dots, x_n] \end{tikzcd}$$
   now take $f \neq 0$ an irreducible polynomial in $q \cap k[x_1, \dots, x_n]$, which we know is prime so we can do this decomposition into irreducibles. Now look at $Spec(R/(p, f))$, then we claim that one of the irreducible components there will contain $Spec(R/q)$. What do we need to make this work?

   Want: $\pi(Spec(R/q)) \neq Spec(k[x_1, \dots, x_n])$. Then the lying over theorem will give us the desired extra prime ideal. Consider $(p, f) \in R$ where $f \not\in np$. Let $p_1, \dots, p_k$ be the minimal primes containing $(p, f)$. Then we want to show
   $$\dim R/p_i = n - 1$$
   $$\exists i \text{ s.t. } q \supsetneq p_i \supsetneq p$$
   In order to get this, we need prime avoidance:

   (d) **Proposition:** (Prime Avoidance) Suppose we have $p_1, \dots, p_k$ prime ideals of a ring $S$. $q$ is a prime ideal and $q \supseteq p_1 \cap \dots \cap p_k$. THEN $q \supseteq p_i$ for some $i$.

   If otherwise, choose $f_i \in p_i \backslash q$ for all $i$. Then the goal is to produce $f \in p_1 \cap \dots \cap p_k$, NOT in $q$. Ravi leaves this for us. □

   (e) Pictorially with the correspondence between closed subsets and prime ideals: $Z(q)$ an irreducible, closed subset is contained in the union of the irreducible closed subsets corresponding to $Z(p_1)$, ..., $Z(p_k)$. THEN $Z(q) \subseteq Z(p_i)$ for some $i$ by irreducibility.

9. **Theorem:** (Going Down) (for integral, closed domain): Suppose $\phi : R \to S$ is a finite ring extension, of integral domains and $R$ is integrally closed. Given prime ideals $p \subset p'$ of $R$ and $q'$ of $S$ with $R \cap q' = p'$, then there exists $q \subset q'$ such that $R \cap q = p$.

10. Ravi says that the proof uses Galois theory and so we'll sidetable this for later

11. Nakayama's lemma

    (a) Version 1: Suppose $R$ is a ring, $I \subseteq R$ is an ideal $M$ is a finitely generated $R$-module and $M = IM$, then $\exists f \in R$ with $f \equiv 1(\mod I)$ for which $fM = 0$

    (b) Here's a non-example, $R = \mathbb{Z}$, $I = (2)$, and $M = \mathbb{Q}$, then $M = IM$, but of course $M$ is not finitely generated so Nakayama's lemma doesn't apply

    (c) The proof boils down to the adjugate trick we've seen before

(d) **Proof:** (of Nakayama): Choose generators $m_1, \dots, m_n$ of $M$, then because $M = IM$, we have

$$m_i = \sum_{j=1}^{n} a_{ij} m_j \quad \text{s.t.} \quad a_{ij} \in m_j$$

Then we have

$$Id \begin{pmatrix} m_1 \\ \dots \\ m_n \end{pmatrix} = \begin{pmatrix} & & \\ & a_{ij} & \\ & & \end{pmatrix} \begin{pmatrix} m_1 \\ \dots \\ m_n \end{pmatrix}$$

and so we get that

$$\det(Id - (a_{ij})) \begin{pmatrix} m_1 \\ \dots \\ m_n \end{pmatrix}$$

by swinging things over to the left and then multiply both sides by the adjugate. Let

$$f = \det(Id - (a_{ij})) = 1 + g, \quad \text{s.t.} \quad g \in I$$

where we get that $f = 1 + g$ by looking at $Id - a_{ij}$ and expanding the determinant. □

(e) Ex: (Nakayama lemma Version 2) If $I \subset \bigcap_{m \text{maximal}} m = J =$ jacobson radical, then $f$ is invertible in $R$ and hence $M = 0$. This is because $(f)$ is not contained in any maximal ideal (if it was, we get a contradiction) and so $(f) = (1)$, meaning that $f$ is invertible

(f) (Version 3) Suppose that $I \subseteq J = \cap_m m$. If $M$ is a finitely generated $R$-module and $N$ is a submodule of $M$. Then if

$$N/IN \to M/IM$$

is surjective, THEN in fact $N = M$. This is an exercise

(g) (Version 4) Suppose $R$ is a local ring with maximal ideal $m$. If $M$ is a finitely generated $R$-module and $\{\overline{x_1}, \dots, \overline{x_n}\}$ generate $M$ modulo $m$, i.e.

$$\overline{x_1}, \dots, \overline{x_n} \in M/mM$$

are basis elements for the vector space $M/mM$, then any choice of representatives for $x_i$ will generate $M$.

(h) Ravi claims that Nakayama's lemma is very geometric because modding out by a maximal ideal is like evaluating at a point in *Spec*.

## 2/12/20

1. Our plan for the rest of the quarter is to discuss discrete valuation rings (which are krull dimension 1), as well as Artinian Rings (krull dimension 0), as well as trace, norm, Going-Down theorem, and rep theory

2. Prime Avoidance (Revisited)

   (a) **Theorem:** Suppose $I \subset R$, $p_1, \dots, p_n$ are prime, and $I \subseteq \bigcup_i p_i$ then $I \subseteq p_i$ for some $i$.
   **Proof:** Suppose $I \not\subset p_i$ for all $i$, want $I \not\subset \cup_i p_i$. So $\exists f_i \in I \backslash p_i$, then we can produce a function $f$ that's a multiplicative combination of these such that $f \not\equiv 0 \mod p_i$ for all $i$. But it's definitely contained in the ideal

3. Note that the above is the actual statement of prime avoidance, not the thing we did last time

4. We know about integral morphisms:

$$\begin{tikzcd} Spec(S) \arrow[d] & q \subset S \\ Spec(R) & p \subset R \arrow[u, "\phi \text{ integral}"'] \end{tikzcd}$$

   If the above diagram holds, then $\dim S/q = \dim R/p$ and $\phi^{-1}(q) = p$.

5. From last time, the codimension is the difference in dimensions (for finitely generated algebras over $k$). Then for $q \subset S$ a prime ideal, $p \subset R$ a prime ideal

$$\begin{tikzcd}
S/q & S/q' \arrow[l] & S \text{ an integral domain, f.g. over k} \arrow[l] \\
R/p = k[x_1, \dots, x_n]/p \arrow[u] & k[x_1, \dots, x_n]/(f) \arrow[l] & k[x_1, \dots, x_n] = R \arrow[l] \arrow[u, hook, "\phi"]
\end{tikzcd}$$

here $n = \dim S$ and $p = \phi(q)$ and $f \in p$ is irreducible. The idea is that given $p$ and $q$, we can find a $q'$ and $(f)$ such that this intermediary extension has the same codimension, because quotienting out by $q'$ and $(f)$ should drop the krull dimension by 1 while keeping the containment.

6. Discrete Valuation Rings

   (a) Ravi says Discrete Valuation Ring (DVRs) is a complicated name to a complicated question: the question of orders of poles and zeros

   (b) Think of 28/3, which as a pole of order 1 at the prime ideal 3, or more canonically, $\sin x$, which has a zero of order 1 at 0, so we can divide by $x$ and get $\sin x/x$

   (c) What about more complicated functions like $(x+y)^3/x$? What type of zero/pole does it have at $(x, y) = (0, 0)$. Or even $\frac{x}{y}$?

   (d) The point is that the notion of "order" of a zero is not well defined for these functions, so we have to talk about Specs instead. Order can then be seen geometrically

   (e) Ravi quickly does the example of looking at $(y - x)/x$ in the ring $\mathbb{C}[x, y]/(y^2 - x^3 - x^2)$. Somehow, approaching the point $(0, 0)$ along the two tangent curves there gives different values for the order of the 0 of $(y - x)/x$ - along the positive slope, $y = x$, we have $\lim_{x=y \to 0}(y - x)/x = 0$, while along the negative slope, $y = -x$, the limit is $-2$, which is not a zero

   (f) Suppose $(R/m)$ is a Noetherian local ring. Earlier in the class, we defined the Zariski cotangent to be $m/m^2$. We have
   $$\dim(m/m^2) \geq \dim R$$

   (g) **Definition:** A Noetherian local ring, is a regular ("smooth") if $\dim m/m^2 = \dim R$.

   (h) Ravi says that the word regular is an artifact of the times, and that we should really think of the word smooth

   (i) At this point, it's not obvious how "smoothness" (whatever that means) is related to the dimension of the cotangent space

   (j) **Definition: /Theorem:** Suppose $(R, m)$ is a Noetherian local ring of dimension 1, then TFAE (DVR)

      i. $(R, m)$ is regular, i.e. $\dim_{R/m} m/m^2 = 1$

      ii. $m$ is principal, $m = (t)$, and we call $t$ the uniformizer.

      iii. All ideals of $R$ are $m^n$ for $n \geq 0$ and $(0)$

      iv. $R$ is a PID

      v. $R$ is a UFD

      vi. $R$ is integrally closed

      vii. Given a field $K$, a discrete valuation on $K$ is a group homomorphism that sends $K^\times \twoheadrightarrow \mathbb{Z}$ such that $\nu(x + y) \geq \min(\nu(x), \nu(y))$. The corresponding DVR is the collection of all elements such that $\nu(x) \geq 0$.
      Define the corresponding valuation ring,
      $$\mathcal{O}_v := \{r \in K \mid \nu(r) \geq 0\} \cup \{0\}$$
      and
      $$m = \{r \in K \mid \nu(r) \geq 1\}$$
      why is $m$ maximal? It suffices to show that every element, $x$, of valuation 0 is invertible, but this is because if $\nu(x) = 0$ then
      $$\nu(xx^{-1}) = \nu(1) = 0 = \nu(x) + \nu(x^{-1}) \implies \nu(x^{-1}) = 0$$
      this is our final definition

**Proof:** (i) $\implies$ (ii): Take $u \in m/m^2$, then some $u$ generates $u$ generates $m \mod m \cdot m$. By Nakayama, we have that $u$ generates $m$, meaning that $m$ is principal.

(ii) $\implies$ (i): If $m$ is principal, then $m/m^2$ is principal. If $m = m^2$, then by Nakayama, $m = 0$ and $R$ is a field, which is dimension 0, a contradiction. Also $\dim m/m^2 \leq 1$, because $m$ is principal.

(iii) $\implies$ (i): $m \supset I \supset m^2$, so $I = m$ or $I = m^2$, giving us the dimension statement.

(i) = (ii) $\implies$ (iii): Suppose $I$ is an ideal and $I$ is not one of $\{m^n\}_{n\geq 1}$, then there exists an $n$ such that $m^{n+1} \subseteq I \subseteq m^n$. This means that we either have an $a \in I$ which is of the form $ut^n$ where $m^n = (t^n)$ and $u$ is a unit OR $a = ut^{n+1}$. Then $I = m^n$ or $m^{n+1}$. This follows by principalness.
Something not obvious is why can there not be an $I \subseteq \bigcap_n m^n$? I.e. why is $\bigcap_n m^n = (0)$? This relies on something called the Artin-Rees lemma. Ravi will give this to us later.

$(ii) = (iii) \implies (iv)$: easy.

$(iv) \implies (ii)$: by definition.

$(iv) \implies (v)$: True. PIDs are UFDs

$(v) \implies (vi)$: The fact that UFDs are integrally closed is like the proof of the rational root theorem.

$(i) = (ii) = (iii) = (iv) \implies$ definition of DVR: the valuation will be the power of the uniformizer and we can extend this to the fraction field.

$DVR \implies (i)$: True because this quotient is everything of valuation 1 quotiented out by everything of valuation 2.

7. Next time, we'll prove $(vi) \implies (i)$.

## 2/14

1. We start with the following lemma

2. **Lemma:** For $(R, m)$ a Noetherian local ring, then

$$\bigcap_i m^i = 0$$

   One way to think about this is consider the Spec version. Then a function which vanishes at all orders of a point, i.e. $m$ in the Spec, must be 0 by analyticity/holomorphic case. The reason we can use holomorphicity and not just smoothness is that the ring of smooth functions is not Noetherian, whereas the ring of holomorphic functions is Noetherian.

3. **Theorem:** $(R, m)$ a Noetherian local ring, also a regular ring ("smooth"), AND $\dim m/m^2 = \dim R$, THEN $R$ is an integral domain

4. **Theorem:** Suppose $(R, m)$ Noetherian, local ring of dimension 1, then TFAE
   (a) $R$ is regular, i.e. $\dim m/m^2 = 1$
   (b) $m$ is principally generated, $m = (u)$ where $u$ is the uniformizer
   (c) All ideals are of the form $m^n$, or $R$, or $(0)$
   (d) $R$ is a PID
   (e) $R$ is a UFD

(f) $R$ is integrally closed

(g) $R$ is a DVR, i.e. there exists $\nu : K(R)^\times \to \mathbb{Z}$ group homomorphism, surjective such that $\nu(x+y) = \min(\nu(x), \nu(y))$

Ravi emphasize that $m/m^2$ should be thought of as a cotangent space, and that this can be used to prove things like the previous theorem. Now we prove $f \implies b$, which was the last thing left to do from last class:

**Proof:** Assume $(f)$ (integrally closed and hence an integral domain). We know $m \neq m^2$, else $m = 0$ by Nakayama and $R = R/m$ a field, then the dimension is not equal to 1. So $m \neq m^2$. Now choose $r \in m/m^2$. Our goal is $M = (r)$. Consider $R/(r)$, which is Noetherian and dimension 0 (this follows because $R/(r)$ is still a local ring with $m$, and $R$ is an integral domain, so the chain of length 2 will be $(0) \subseteq m$, thus when passing to the quotient we must be dimension 0). Now, $R/(r)$ has a maximal ideal, $n$, which is also the nilradical (intersection of all maximal ideals). We have a diagram

$$\begin{tikzcd}
R/(r) & \left[n\right] \arrow[d] \\
R \arrow[u, "\phi"] & \{[m], [(0)]\}
\end{tikzcd}$$

We further have that $n^N = 0$ for some $N$, which holds because $n$ is finitely generated, say $n = (n_1, \ldots, n_q)$. This means that

$$m^N = 0 \mod (r) \implies (r) \supseteq m^N$$

in our original ring, $R$. Choose $N$ smallest so that the above holds. We hope that $N = 1$. Let $s \in m^{N-1} \backslash (r)$, then we have that

$$\frac{s}{r} \in K(R), \qquad \frac{s}{r} \notin R \implies \frac{s}{r}\text{not integral over R}$$

Recall this FACT: If we have a finitely generated $R$-module, $M$ with faithful $R[\alpha]$-action, THEN $\alpha$ is integral over $R$, where $\alpha \in K$ and $K$ is the fraction field of $R$. From here, we want our $M$ to be one of the ideals we've described so far.

Now note that $sm \subseteq (r)$, i.e. $m \subseteq \frac{s}{r}R$. In other words, $m$ is an $R\left[\frac{s}{r}\right]$ module, and so $\frac{s}{r}$ must be integral over $R$, a contradiction. □

5. To clarify the above, we're consider $m$ and $R[\frac{r}{s}]m$ as submodules of $K(R)$, the fraction field of our integral domain. Multiplication never has a kernal when we're inside a field, and so we get faithfulness of the action

6. As an aside, Ravi says that this fact is the main use of being integral closed

7. We now start a new topic, Dedekind Domains

8. Dedekind Domains

   (a) **Definition:** A dedekind domain is a Noetherian integrally closed domain of dimension 1

   (b) e.g. $\mathbb{Z}$, $k[t]$, any $DVR$, the $p$-adics, the ring of integers in a number field. This last one is the integral closure of $K$, where $K$ is some finite extension of $\mathbb{Q}$, over $\mathbb{Z}$

$$\begin{tikzcd}
\text{integral closure over } \mathbb{Z} \arrow[r, hook] & K \\
\mathbb{Z} \arrow[u] & \mathbb{Q} \arrow[u, "finite"]
\end{tikzcd}$$

   The ring of integers is the top left. The integral closure of something over $\mathbb{Z}$ is integrally closed, an integral domain, and by the going up theorem, it will be dimension 1. But there's a little work to show that the ring of integers is Noetherian...

   (c) Again, we consider $k[x,y]/(y^2 - x^3 + x)$, which is a Dedekind domain, because its the Integral closure of the above ring but if we added another variable $z$ such that $z^2 - x^3 + x$.

(d) **Lemma:** Dedekind domain is equivalent to being Noetherian, dimension 1, and all of the local rings $R_m$ for maximal $m$, are in fact DVRs.

**Proof:** To see this, recall that an integral domain $R$ is integrally closed iff $R_m$ is integrally closed for all $m$ maximal. One direction is easy, the other direction is as follows: Suppose we have $x \in K(R)$ such that $x \notin R$ but $x$ is integral over $R$. Then consider $I \subset R$ such that

$$I = \{r \ : \ rx \in R\}$$

This is an ideal with $1 \notin R$, and hence is contained in some maximal ideal $m$. This will give that $x$ is integral over $R_m$, but not contained in $R_m$ a contradiction.

Also recall: for $R$ an integral domain that $R \hookrightarrow K = K(R)$ where

$$R = \bigcap_{p \text{ prime}} R_P = \bigcap_{m \text{ max}} R_m$$

Translation: We have $\bigcap_m R_m \subset R$ already. If $x \in \bigcap R_m$, then we define

$$I = \{r \mid rx \in R\}$$

If $I = (1)$, then $x \in R$ and we're done. Else $I$ is contained in some maximal element, $m$, and we see that $x \notin R_m$, a contradiction. These two facts give us te equivalence of definitions of Dedekind domains. □

(e) For a Dedekind domain, $R$, take $0 \neq x \in K(R)$. It has some order of zero or pole at every maximal ideal. Any element of $K$ is in $R$ if and only if all of its discrete valuations are $\geq 0$

(f) **Proposition:** Every PID which is not a field, is a dedekind domain.

**Proof:** We nee to show that $\dim R = 1$. If we have this, we know that all localizations are DVRs because of the equivalence in our big theorem from the beginning of class.

If $R \supset p \supset (0)$, then we want to show that $p$ is maximal. But all prime ideals in a PID are maximal. Formally, let's look at $R/(p)$, then if this is not a field, take $s \in R/(p)$, we want to show that it is invertible, i.e. $(s, p) = (1)$. Suppose not, then $(s, p) = (q)$ for some $q$ not a unit. Then $p = rq$ where $p$ is prime. If $r \in (p)$, then we have

$$p = rq = (ps)q \implies p(1 - sq) = 0 \implies 1 = sq$$

so $q$ is a unit. Else, we would have that $q \in (p)$, which contradicts the choice of $s \neq 0$ as an element of $R/(p)$. □

(g) We know that PIDs are UFDs, and we've just shown that PIDs are Dedekind domains. Are Dedekind domains UFDs? No

# 2/17/20

No class because of president's day

# 2/19/20

1. We're going to finish commutative algebra today

2. We've been talking about discrete valuation rings, and now we'll move the conversation to Dedekind domains, which have a lot of corresponding properties

3. Dedekind Domains

   (a) **Definition:** A Dedekind domain is a Noetherian integrally closed integral domain of dimension 1

   (b) Recall that if $R$ is an integral domain, then

$$R = \cap_{m \text{ maximal}} R_m$$

(c) Rmk: a Dedekind domain is equivalently a Noetherian integral domain of dimension 1 such that all maximal ideals give $R_m$, a DVR

(d) Because of this, we can talk about the order of vanishing of each $P \in Spec(R)$ by looking at $R_m$ for $m \supseteq P$

(e) **Proposition:** If $R$ is a principal ideal domain, then $R$ is a Dedekind domain

(f) Aside: what is a Dedekind domain that's not a UFD? How about a UFD that's not a Dedekind domain?

4. Fractional Ideals

   (a) Suppose $R$ is an integral domain (likely a Dedekind domain), define the fractional ideal to be

   $$M \subseteq K(R)$$

   for $M$ a sub $R$-module of the $R$ module, $K(R)$, such that there is some $d \in R\backslash\{0\}$ such that $dM \subseteq R$. This means that $M$ has elements which have "bounded denominators"

   (b) Principal fractional ideal, $dR$ where $d \in K(R)^{\times}$

   (c) Ex: of fractional ideals of $\mathbb{Z}$, principal ideals like $\mathbb{Z}\left[\frac{3}{175}\right]$

   (d) Question: What are the fractional ideals of $\mathbb{Z}$? We know that

   $$dM \subseteq \mathbb{Z}$$

   for some $d$, but $dM$ is also an ideal in $\mathbb{Z}$, so it is principally generated, i.e. $dM = (a) \subseteq \mathbb{Z}$, so that

   $$M = \frac{a}{d}\mathbb{Z}$$

   (e) **Definition:** Multiplying fractional ideals, $J_1$, $J_2$, is notated by $J_1J_2$ and this is a fractional ideal as

   $$d_1J_1 \subseteq R, \qquad d_2J_2 \subseteq R \implies (d_1d_2)(J_1J_2) \subseteq R$$

   because $R$ is commutative

   (f) **Definition:** $J_1$ is an invertible fractional ideal if there exists a $J_2$ such $J_1J_2 = R \subseteq K(R)$

   (g) Ex: All principal fractional ideals are invertible, because

   $$(eR)(e^{-1}R) = R, \qquad e \in K(R)^{\times}$$

   (h) Remark: The invertible fractional ideals form a group. The principal fractional ideals form a subgroup

   (i) **Definition:** The class group is defined to be

   $$Cl(R) = \{\text{invertible fractional ideals}\}/\{\text{principal fractional ideals}\}$$

   (j) **Definition:** The class number is equal to $|Cl(R)|$ (here, we're taking actual cardinality of the set, not rank or anything)

   (k) Ex: If $R$ is a principal ideal domain, then the class number is 1

   (l) Remark: The ring of integers over every number field has finite class number

   (m) Ex: Consider $\mathbb{C}[x,y]/(y^2 - x^3 + x)$ has infinite class number. Somehow the class group of this ring is $\mathbb{R}^2/\mathbb{Z}^2$. Every point on this torus corresponds to some maximal ideal, which gives a fractional ideal of some sort. Moreover, multiplication of two maximal ideals gives another maximal ideal (modulo principal ideals)

   (n) Visually, we can even get the group law for addition of points of elliptic curves through the class group

   (o) If the Class number is 1, then $Cl(R) = \{0\}$, then all invertible fractional ideals are principal, and hence (to be shown) all ideals are principal, which implies that $R$ is a PID

   (p) We're missing the fact that all nonzero ideals are invertible (will be proved soon)

   (q) Another perspective on ideals for dedekind domains

   i. Given a non-zero, fractional ideal, define a corresponding divisor. A divisor for a Dedekind domain, $R$, is a finite formal $\mathbb{Z}$-linear sum of $[m]$, i.e. take the free abelian group on the maximal ideals

ii. Ex: an element could look like $3[m_1] - 2[m_2]$, so on $\mathbb{Z}$, we might have something like $3[(5)] - 2[(3)]$

iii. **Definition:** The divisor group is the group of all divisors as above. An effective divisor is something where all the coefficients are non-negative.

iv. Remark: We'll represent a generic element by $\sum_i a_i p_i$ where the $p_i$ is an equivalence class of maximal ideals

v. Any nonzero, $\alpha \in K(R)$, we can define $div(\alpha)$ to be the formal sum of all the maximal ideals where the coefficient will be the valuation of $\alpha$ in the localization $R_m$

vi. Ex:

$$div(27/175) = div(3^3/(5^2 \cdot 7)) = 3[(3)] - 2[(5)] - [(7)]$$

Then $div(\alpha)$ is effective iff $\alpha \in R$. Moreover $div(\alpha) = 0$ if and only if $\alpha$ is a unit in $R$

vii. Hence, the semigroup of effective divisors, is

$$\{R\backslash\{0\}, \times\}/\{\text{units}\}$$

i.e. all the non-zero elements of $R$ mod units.

viii. Formally

$$div(\alpha) = \sum_{m \text{ maximal}} val_m(\alpha)$$

how do we know that this sum is finite?

**Proof:** $R/(r)$ is dimension 0 (quotienting by $(r)$ strips off the prime ideal (0) from our chain). Thus $Spec(R/(r))$ has finitely many irreducible components, because $R/(r)$ Noetherian which forces any Zariski closed subset to have finitely many irreducible components. Thus $R/(r)$ has finitely many minimal primes

ix. **Proposition:** If $S$ is a Noetherian dimension 0 ring, then $S$ has finitely many prime ideals, all maximal. See here

`https://math.stackexchange.com/questions/771412/noetherian-ring-of-krull-dimension-0`

x. Ex: $\mathbb{C}[x, y]$ and the ideal $(y^2 - x^3 + 2x)$, then something about looking at $\frac{(y-2)}{(x-2)}$ and how this has order 0 at the maximal ideal $(x - 2, y - 2)$.

xi. **Theorem:** Suppose $R$ is a Dedekind domain, then TFAE (A)

A. Effective divisors of $R$

B. Ideals of $R$

TFAE (B)

A. Divisor

B. Invertible fractional ideal

C. (non-zero) fractional ideals

**Proof:** (A) Given a non-zero ideal, create the divisor:

$$div(I) = -\inf\left(div_{r \in I\backslash\{0\}} r\right) = -\sum_{m \text{ max}} \left(\min_{r \in I\backslash\{0\}} val_m(r)\right)[m]$$

e.g the minimum between (175) and (30) would be $[(5)]$ because $div(175) = 2[(5)] + 1[(7)]$ and $div(30) = [(2)] + [(3)] + [(5)]$, so taking the minimum of each coefficient, we get $[(5)]$.
Given a divisor $D = \sum_i a_i p_i$, then define

$$I_D = \{r \in R \, : \, val_{p_i} \geq a_i\} \cup \{0\}$$

e.g. $D = [(2)] + 3[(5)]$ in the divisor group of $\mathbb{Z}$, then $I = (250)$.
To what extent is this a bijection? We have a map ideals → div → ideal where

$$J \mapsto div(J) \mapsto I_{div(J)}$$

where $J_{div(I)}$ is the ideal generated by $div(I)$. We definitely have $J \subset I_{div(J)}$. Given $\alpha \in I_{div(J)}$, is it in $J$? For any $\beta \in J\backslash\{0\}$, we have

$$val_P(\alpha) \geq val_P(\beta)$$

for all but finitely many $P$. For any $p$, there exists $\beta_P \in J \backslash \{0\}$ such that $val_P(\alpha) \geq val_P(\beta_P)$, **so** there exists $\beta_1, \dots, \beta_n$ with $val_P(\alpha) \geq val_P(\beta_i)$ for some $i$. **So** $(\beta_1, \dots, \beta_n) \subseteq J$, and we'll see (next time)that

$$\alpha = \gamma_1\beta_1 + \cdots + \gamma_n\beta_n$$

Alternatively, (without a particular $\alpha$ in mind), we can find $\beta_1, \dots, \beta_n \subseteq J$ with $div(\beta_1, \dots, \beta_n) = div(J)$ and hence (somehow)

$$(\beta_1, \dots, \beta_n) = J$$

(B) How do we show this

xii. Note: divisor of an ideal is effective.

xiii. Note: If $div(I) = 0$, then $I = R$ because for every maximal ideal, $I$ contains an element not in that maximal ideal, but if $I$ is contained in some maximal ideal, then this is a contradiction

xiv. After this, we'll see that every non-zero ideal is a unique product of powers of maximal ideals

xv. This gives a unique factorization of ideals

## 2/21/20

1. On the current problem set, we should interpret "$Spec(R)$ is normal" as $R$ is integrally closed

2. Also on the current problem set, Ravi will fix problem 3 because not all of the conditions are there

3. Back to Dedekind domains

   (a) They are Noetherian, dimension 1, integrally closed domains

   (b) We ask when is a Dedekind domain a PID? There are a few criterion for this

   (c) DVRs are PIDs, so any localization of a Dedekind domain is a DVR and hence a PID

   (d) In DVRs, non-zero ideals correspond to $\mathbb{Z}^{\geq 0}$ because $I = (t^n)$ for some $n \geq 0$ and $t$ a uniformizer

   (e) Fractional ideals correspond to the indices $\mathbb{Z}$ in a Dedekind domain because we're allowed negative powers, i.e. $t^nR$, which is considered as a module

   (f) Dedekind domains are more general, and have a group of divisors

   $$div(f) = \sum_{P \text{ prime}} val_P(f) \cdot [P]$$

   (g) The divisor of a nonzero fractional ideal is

   $$\min_{f \in I \backslash \{0\}} (div(f)) = \sum_P \min_{f \in I \backslash \{0\}} (val_P(f)) \cdot [P]$$

   (h) We want to exclude things like $\mathbb{Z}_{\{2^n\}}$, i.e. the submodule of $\mathbb{Q}$ where we allow denominators of any power of 2, because then the divisor of this $\mathbb{Z}$-module has infinite coefficient for $P = (2)$.

   (i) Effective divisors: divisors which have non-negative coefficients and all but finitely many coefficients are 0

   (j) We have a map from ideals to divisors, $J \mapsto div(J)$ as before

   (k) Also have the inverse map

   $$D \mapsto I(D) = \{r \in R \mid div(R) \geq D\}$$

   where the inequality holds for every coefficient

   (l) Claim: These two maps give a bijection, and we'll prove that ideals correspond to effective divisors

   (m) **Proposition:** In a Dedekind domain $R$, an element $g \in (f_1, \dots, f_n)$ if and only if $div(g) \geq \min_i div(f_i) = div((f_1, \dots, f_n))$

**Proof:** The forward direction is nice: if $g \in (f_1, \dots, f_n)$, we have

$$g = \sum_i a_i f_i, \qquad div(g) = div\left(\sum_i a_i f_i\right) \geq \min_i(div(a_i f_i)) = \min_i[div(a_i) + div(f_i)] \geq \min_i div(f_i)$$

The first inequality follows by looking at each valuation and then noting that $\nu(f+g) \geq \min(\nu(f), \nu(g))$. The later inequality uses additive of valuations when two elements are multiplied and that $div(a_i) \geq 0$ because $a_i \in R$.

For the other direction, we do induction on $n$. Base case: $g \in (f)$, in which case $\div(g) \geq div(f)$ because

$$\frac{g}{f} \in R \implies div(g/f) = div(g) - div(f) \geq 0$$

Now given $div(g) \geq \min_{i \leq n}(div(f_i))$, want $g \in (f_1, \dots, f_n)$. In particular, we want to find $a_n$ such that

$$div(g - a_n f_n) \geq \min_{i \leq n-1}(div(f_i))$$

Question: For which $P$ is

$$min_{i \leq n}(val_P(f_i)) \neq \min_{i \leq n-1}(val_P f_i)$$

i.e.

$$val_P(f_i) \leq \min_{i \leq n-1}(val_P(f_i))$$

To get this formally, there exist finitely many $p$ with

$$val_p((f_1, \dots, f_{n-1})) > val_P(g) \text{ and } val_p((f_1, \dots, f_{n-1})) \geq val_P(f_n)$$

want an $a$, independent of $p$ with

$$val(g - af_n) \geq val_P(f_1, \dots, f_{n-1})$$

In $R_p$, this is easy, because we can find $a \in R_p$ with

$$g \equiv af_n \mod P^{val_P((f_1, \dots, f_{n-1}))}$$

which tells us that $val_P(g/f_n)$.
We can find such an $a$ in $R/\prod P^{val_P(f_1, \dots, f_{n-1})}$ by the chinese remainder theorem (using the fact that powers of different maximal ideals). Then taking any representative of $a$, call it $a_n \in R$, will give

$$val_P(g - a_n f_n) \geq \min_{i \leq n-1} val_P(f_i)$$

for all $P$ we chose. For the other prime ideals, we have $val_P(f_n) \geq val_P((f_1, \dots, f_{n-1}))$ and $val_P(g)$ and so adding $a_n f_n$ to $g$ will keep the valuation of $val_P(g - a_n f_n) \geq val_P((f_1, \dots, f_n))$. □

(n) As an example of finding this $a$ element, consider $f_1 = 9 \times 25$, $f_2 = 4 \times 25$, $f_3 = 4 \times 9$, then

$$1 \in (f_1, f_2, f_3)$$

We have $\div((f_1, f_2, f_3)) = 0$, so we should be able to find an $a$ such that

$$1 - a \cdot 36 \in (225, 100)$$

note $div(225, 100) = 2 \cdot [5]$. Note that we can find an $a$ such that $1 - a \cdot 36 \in (5)$. Now square the above expression and we'll get an $\tilde{a}$ such that $1 - \tilde{a} \cdot 36 \in (25)$.

(o) **Proposition:** The divisor map $J \mapsto div(J)$ is surjective, i.e. for all divisors, $D$, there exists a $J$ with $div(J) = D$.

**Proof:** Given an effective divisor $D$, we use chinese remainder theorem twice to construct an element, $\alpha$, such that $div(\alpha) \geq D$, and it coincides with $D$ at all of the primes $P$ for which $val_P(D) \neq 0$. Thus $val_P(\alpha) > val_P(D)$ when $P$ is such that $val_P(D) = 0$. Call these such primes $\{P_i\}$. Then again by chinese remainder, we can find $\beta$ such that $val_{P_i}(\beta) = 0$ and $div(\beta) \geq D$. Then $(\alpha, \beta)$ will have $div((\alpha, \beta)) = D$ by the minimality property of divisors.

## 2/24/20

1. Today: Artinian rings, modules (finite length things)
2. Ravi says we don't have to do problem 3 on the set (the one about $\mathbb{Z}[x]/(x^2-n)$)
3. "Dimension" of a module
   (a) This notion is compared to that of the dimension of something over $k$, a field

   (b) **Definition:** A **simple** module, $M \neq 0$, over $R$ is a module with no non-trivial subobjects, i.e.

   $$0 \subseteq N \subset M \implies 0 = N$$

   (c) Observe, an R-module, $M$ is simple iff $M \cong R/m$ for $m$ maximal.

   (d) The reason for this is: If $M$ is simple, choose any $m \neq 0$ in $M$, then

   $$\phi : R \to M \text{ s.t. } \phi(r) = rm$$

   has non-zero image, and the image is a submodule of $M$, thus $\operatorname{Im}(\phi) = M$, and thus $M \cong R/\ker(\phi)$ for $I \neq R$. Moreover, $I \subseteq m$ for $m$ maximal, so $M = R/I \twoheadrightarrow R/m$. But the image is a field and $M$ is simple, so the kernel of this map must be $M$ or 0. In order for the image to be non-trivial, and hence all of the field, we have that the kernel is 0, so

   $$R/m \cong M$$

   for $m$ maximal. □

   (e) **Definition:** A composition series for an $R$-module $M$ is a finite length chain,

   $$0 = M_0 \subset M_1 \subset \cdots \subset M_{n-1} \subset M_n = M$$

   such that $M_j/M_{j-1}$ is simple

   (f) **Theorem:** (Jordan-Holder) Any two finite composition series for $M$ have the same length, and they have isomorphic quotients, $M_j/M_{j-1}$, up to permutation of the quotients.
   **Proof:** Given two series

   $$M_0 = 0 \subset M_1 \subset \cdots \subset M_n = M$$
   $$N_0 = 0 \subset N_1 \subset \cdots \subset N_m = M$$

   then we can form a table

   $$\begin{pmatrix} & M_0 & M_1 & \dots & M_n \\ N_0 & 0 & 0 & \dots & 0 \\ N_1 & 0 & & & \\ \dots & \dots & & N_i \cap M_j & \\ N_m & 0 & & & \end{pmatrix}$$

   So every entry is the intersection of the two initial modules at the top of the row/ column. In particular, zooming into a particular into a particular $2 \times 2$ subsystem, we have the following cases

   $$\begin{pmatrix} B \cap C & B \\ C & A \end{pmatrix}, \quad \begin{pmatrix} A & A \\ A & A \end{pmatrix}, \quad \begin{pmatrix} B & B \\ A & A \end{pmatrix}, \quad \begin{pmatrix} B & B \\ B & A \end{pmatrix}$$

   If we draw lines blocking out the $A$'s, then we get that the quotient of $A$ and the module above or to the left of $A$ are isomorphic to the remaining modules mod each other, e.g.

   $$\begin{pmatrix} B \cap C & B \\ C & A \end{pmatrix}, \qquad A/C \cong B/B \cap C, \quad \text{and} \quad A/B \cong C/C \cap B$$

   this follows because $A/B$ and $A/C$ are simple and $B \neq C$ (else we wouldn't have labeled them differently). We do the following tiling: we start on the bottom-most row and then draw an edge to the left of the current square iff

   $$(\textbf{current square})/(\textbf{square to the left}) \cong (\textbf{square above})/(\textbf{square to the above and left})$$

Repeating this, we'll eventually reach a point at which this doesn't hold (because top row is 0), and in fact the quotient of the square above by square above and to the left will be 0. At this point, we move to the right and draw edges which indicate that

$$(\textbf{current square})/(\textbf{square above}) \cong (\textbf{square to the right})/(\textbf{square to the right and aobve})$$

Such a procedure gives a bijection between the bottom row, $N_m \cap M_i = M \cap M_i = M_i$ and the right most column, $M_n \cap N_j = M \cap N_j = N_j$ in the sense that it tells us $M_i/M_{i-1} \cong N_j/N_{j-1}$ by comparing these modules and the quotients of the module to left/above and following the chain of equal quotients. □

(g) **Definition:** The length of a module is defined to be the length of any composition series

(h) Remark: Length is additive in exact sequences, i.e.

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

Then lengths of $M'$ and $M''$ add to the length of $M$. In particular, if $M' \hookrightarrow M$, then $length(M') \leq length(M)$

(i) **Definition:** A module satisfying the descending chain condition is Artinian.

(j) Observe: finite length modules are Artinian AND Noetherian

(k) Geometric Intution: Consider $V(y-x^2)$ and $V(y)$, which correspond to the rings $\mathbb{C}[x,y]/(y-x^2)$, $\mathbb{C}[x,y]/(y)$. To get some geometric perspective, suppose we wanted to calculate the dimension of the intersection of the above two varieties, then we look at

$$\mathbb{C}[x,y]/(y-x^2,y) \cong \mathbb{C}[x]/(x^2)$$

which is a length 2 module over $\mathbb{C}$, indicating that the multiplicity at $(0,0)$ in $V(y-x^2) \cup V(y)$ is 2. In general, if we want to calculate the vanishing degree of a point on the intersection of $V(f)$ and $V(g)$, then we look at $\mathbb{C}[x_1,\dots,x_n]/(f,g)$ and calculate the length of this module. The joint quotient module actually gives us more information, but we'll get into this later

(l) **Definition: /Theorem:** A ring $R$ is Artinian if it satisfies the following equivalent statements

i. It is a finite length module over itself
ii. It satisfies the descending chain condition for ideals
iii. It is a Noetherian ring of dimension 0
iv. It is a finite product of Noetherian local rings of dimension 0

**Proof:** From the earlier remark, $(i) \implies (ii)$. For intuition on (iii), note that it says there are finitely many points in the spectrum, and hence (iv) should follow if we write the ring as some product of localizations. We now prove some lemmas which will help us with the proof of this theorem

(m) **Lemma:** $R$ DCC implies finitely many maximal ideals.
Otherwise $\{m_1,\dots,m_n,\dots\}$ and we can form

$$m_1 \supsetneq m_1 \cap m_2 \supsetneq m_1 \cap m_2 \cap m_3 \supsetneq \dots$$

This is strictly decreasing because $m_1 \cap \cdots \cap m_n \supsetneq m_1 \cap \cdots \cap m_{n+1}$, BECAUSE

$$\exists r \in R \text{ s.t. } r \equiv 0 \mod (m_1 \cdots m_n), \quad r \not\equiv 0 \mod m_{n+1}$$

which follows from the chinese remainder theorem or looking at the spectrum of this ring. □

(n) **Lemma:** DCC implies $\cap_p p = \cap_m m$, i.e. the nilradical equals to jacobson radical.
**Proof:** We definitely have $\cap m \supseteq \cap p$. Now take the jacobson radical, $J$, and

$$J \supset J^2 \supset J^3 \supset \dots$$

This is a descending chain so $J^k = J^{k+1}$ for some $k$. Nakayama's lemma then tells us that $J = 0$, so the jacobson radical is contained in the nilradical. Nakayama uses finitely generated, so let's consider

$$x \in J, \qquad (x) \supset (x^2) \supset (x^3) \supset \cdots \implies \exists k \text{ s.t. } (x^k) = x(x^k)$$

this is from the DCC. Now note that $x \in J$, so $x$ is in any maximal ideal $m$, thus $(x^k) = m(x^k)$ and we can apply Nakayama's lemma to this finitely generated module, so $(x^k) = 0$, which implies that $x^k = 0$, so every element in the Jacobson radical is in the nilradical. □

(o) **Lemma:** DCC implies $\dim R = 0$.

**Proof:** Suppose $Q$ is prime but not maximal. Then from before

$$\cap_p p = \cap_m m \implies (\cap_p p) = (\cap_p p) \cap Q = \cap_m m = (\cap_m m) \cap Q$$

BUT we can find an $f \in R$ such that $f \in m_1 \cdots m_n$ but $f \notin p$ (this uses DCC somehow, but we skip over the details). □

(p) **Lemma:** DCC implies $R = \prod_{m \text{ maximal}} R_m$. In particular, we can whip up an isomorphism $R \to \prod_{m \text{ max}} R_m$

(q) **Lemma:** For $R$ satisfying the DCC, $m/m^2$ is finite dimensional as an $R/m$-vector space.

**Proof:** This isn't bad, if $m/m^2$ is infinitely dimensional, then we could find an infinite decreasing chain $m \supsetneq m_1 \supsetneq m_2 \supsetneq \dots$ never reaching $m^2$. This would contradict the DCC condition. □

(r) **Lemma:** : Reduce to the case when $R$ is local, choose a basis for $m/m^2$, lift this basis to $R$, then it generates $R_m$.

## 2/26/20

1. Ravi says that for problem 7 on this week's HW, we should use that an algebra finitely generated over a field is catenary to get invariance of the dimension in terms of the maximal ideal we choose in it. Might also need to use the fact that dimension equals transcendence degree of the field of fractions

2. Ravi says that in order to understand things like the Artin Rees Lemma or Nakayama's lemma, it's useful to change our intuition/perspective

3. For Nakayama: think about $R/m$, Nakayama's lemma tells us that if we understand something to 0th order then we understand it fully

4. Last Time:

   (a) A module is seen as some simple object

   (b) We discussed composition series and Jordan-Holder theorem

   (c) This gives us the notion of a finite length module

   (d) Artinian Rings: we had equivalent definitions

      i. DCC on ideals

      ii. finite length module over itself

      iii. Noetherian ring of dimension 0

      iv. Finite product of Noetherian local rings of dimension 0

   (e) Note: A Noetherian local ring of dimension 0 is called an Artin local ring

   (f) Note: DCC on $R$ implies that $R/I$ and $R_m$ satisfy the DCC

   (g) Note: DCC implies finitely many maximal ideals

   (h) Note: DCC implies that $\cap_m m = \cap_p p$

   (i) Note: DCC implies that our ring is dimension 0, else we would get a prime ideal that is not maximal, meaning that $\cap_m m \neq \cap_p p$ because secretly $\cap_m m = \cap_{i=1}^n m_i$ and we could find an element $x \in \cap_{i=1}^n m_i \backslash p$.

   (j) Problem set question: DCC implies that $R = \prod_{i=1}^n R_{m_i}$, i.e. the embedding $R \to \prod_i R_{m_i}$ is an isomorphism. The reason is that $R \to R_m$ is surjective and the kernels of these maps are comaximal, i.e. $\ker(R \to R_{m_1}) + \ker(R \to R_{m_2}) = R$. Note that

   $$\ker(R \to R_m) = \{x \in R \mid \exists \ell \in R \backslash m \text{ s.t. } \ell \cdot x = 0\}$$

   The goal is to find $x$, $y$ such that $1 = x + y$ and

   $$\ell_1 x = 0, \quad \ell_2 y = 0, \qquad \text{s.t. } \ell_1 \notin m_1, \ \ell_2 \notin m_2$$

(k) Assuming the problem set question, we get that $R = \prod R_m$, where each is a local DCC Artinian ring

(l) $(R, m)$ is local DCC implies that $m/m^2$ is a finite dimensional vector space over $R/m$. For the same reason $m^n/m^{n+1}$ is finite dimensional. Moreover by DCC, we have $m^n = 0$ for some $n$, meaning that $m$ is a finitely generated $R$-module, and so $R_m$ is Noetherian. To see that $m^n = 0$ for some $n$, we push this until later...

(m) Note: A finitely generated module is **not** necessarily noetherian. It is true that a finitely generated module over a noetherian ring is noetheriean because every such module is of the from $R^n/I$ for some $n$ and $I$ an ideal

(n) Most of the pieces are here, but Ravi will come back to this later

5. Now we move to representation theory

(a) $G$ a finite group

(b) Fix a field $k$ (usually char 0, usually algebraically closed)

(c) Consider finite dimensional vector spaces over $k$

(d) **Definition:** A representation of $G$ of a vector space, $V$, is a map $\rho : G \to GL(V)$

(e) Let $V \in Rep_G$, then $V \xrightarrow{g} V$.

(f) **Definition:** The group algebra, $k[G]$, or $kG$ is the collection of all elements $\sum_{g\in G} \alpha_g[g]$ where $\alpha_g \in k$ and such that $[g] \cdot [h] = [gh]$

(g) Note that the group algebra is a non-commutative $k$-algebra, however it is Artinian

(h) Note that if $G$ is abelian, then $k[G]$ is commutative, and in general, $k[G_1 \times G_2] \cong k[G_1] \otimes k[G_2]$

(i) In particular $k[\mathbb{Z}/n\mathbb{Z}] \cong k[x]/(x^n - 1)$, so the structure theorem for finitely generated modules over a PID will give $k[G] \cong$ products of rings like this

(j) There's some remark about the Hopf algebra, which makes the spectrum of the ring into a more algebraic structure

(k) $V$ is a finitely dimensional representation of $G$ if and only if $V$ is a $k[G]$-module which is finitely generated

(l) The center of $k[G]$

i. Consider something in the center $\sum_i \alpha_i[h_i]$, then we have

$$[g]\sum_i \alpha_i[h_i] = \sum_i \alpha_i[h_i][g] \implies \sum_i \alpha_i[gh_i] = \sum_i \alpha_i[h_i g]$$

Thus $\sum_i \alpha_i[h_i]$ is in the center if and only if $\alpha_i$ depends only the conjugacy class of $h_i$.

ii. Thus, the center gives a commutative subalgebra, and we can look at its spectrum

iii. I ask if non-commutative rings have spectrum, Ravi says yes but it gets messy

iv. Consider $G = S_3 = \{e, (1\ 2), (2\ 3), (3\ 1), (1\ 2\ 3), (2\ 3\ 1)\}$. Then we have that the center is spanned by

$$1 = (e), \qquad s = [(1\ 2)] + [(2\ 3)] + [(3\ 1)], \qquad t = [(1\ 2\ 3)] + [(1\ 3\ 2)]$$

then the center is the algebra

$$\mathbb{C}[s,t]/(s^2 + 3 + 3t,\ t^2 = 2 + 2t,\ st = 2s)$$

This tells us that $s = 0$ or $t = 2$. We solve for the solutions of this system of equations and get $(0, -1)$, $(2, 3)$, $(-2, 3)$, and these correspond to the irreps: trivial, alternating, and standard

v. Ravi says that we can systematically construct the irreps from points in the spectrum and vice versa. Cool!

## 2/28/20

1. Talking about representations again: given a group $G$ and a field $k$, a representation of $G/k$ is a map $\rho : G \to GL(V)$ where $V$ is a $k$-vector space.

2. Ex: The trivial rep, where everything in $G$ acts by the identity

3. A representation is faithful if only $e \mapsto Id = \rho(e)$ and all other group elements give non-trivial elements of $GL(k^n)$. A faithful representation can be embedded into $GL(k^n)$ and so can be considered as a matrix representation

4. Other examples: the dual of a representation, the determinant on $\wedge^n V$ and $Sym^k(V)$. Can also build reps using $\oplus$ and $\otimes$

5. **Definition:** The degree of the representation is the dimension of the vector space the homomorphism maps into

6. **Definition:** A morphism of $G$ representations is a map $\phi : V \to W$, both $G$-reps such that

$$\begin{tikzcd} V \arrow[r, "\phi"] \arrow[d, "\rho(g)"] & W \arrow[d, "\sigma(g)"] \\ V \arrow[r, "\phi"] & W \end{tikzcd}$$

7. Note that $\text{Hom}_G(V, W)$ (i.e. all $G$-linear homomorphisms) is a vector space, but not a representation. However, $\text{Hom}_k(V, W) \cong W \otimes V^*$ is a $G$-rep, what is the action? It's conjugation, i.e.

$$g \cdot \varphi \mapsto g\varphi(g^{-1})$$

8. **Definition:** The group ring, $kG = k[G]$ is the collection of all form sums, $\sum_g \alpha_g[g]$ for finitely many non-zero coefficients (this is relevant for infinite groups)

9. $G$-representations over $k$ are equivalent to $kG$-modules

10. **Definition:** The regular representation is the representation generated by $G$ acting on $k[G]$

11. Idea: Because every $G$-representation can be considered as a $kG$ module, every irreducible representation is contained in $kG$

12. Remark: Let $\ell/k$ be a field extension, then we have a map $k \to \ell$, and hence a ring map

$$kG \hookrightarrow \ell G$$

and this induces a map $Mod_{\ell G} \to Mod_{kG}$.

13. Remark: Similarly, if we have a map between groups $G \to H$, then we get a map $kG \to kH$ and hence a map the other direction $Mod_{kH} \to Mod_{kG}$.

14. In the particular cases of

$$\{e\} \to G$$
$$G \to \{e\}$$

Note that $Mod_{k\{e\}} = \{\text{vector spaces over } k\}$, and so the induced map from $Mod_{k\{e\}} \to Mod_{kG}$ is that which sends a vector space to a trivial $G$-rep.

15. Representations of finitely generated abelian groups

    (a) We have the following correspondences between groups and group algebras

    $$G = \mathbb{Z}/n \leftrightarrow kG = k[t]/(t^n - 1)$$
    $$G = \mathbb{Z} \leftrightarrow kG = k[t, t^{-1}]$$

    (b) What is a $k[t]$-module? Some copies of $k[t]$ and quotients of it by irreducible polynomials. This follows from the structure theorem for PIDs

    (c) What about finitely generated $k[t, t^{-1}]$ modules? Assume that $k$ is algebraically closed. Then a $k[t, t^{-1}]$ is still a PID (consider it as $k[t]_{(t)}$) and so the modules look like

    $$k[t, t^{-1}]^n \oplus k[t, t^{-1}]/(t - \alpha_1)^{n_1} \oplus \ldots k[t, t^{-1}]/(t - \alpha_m)^{n_m}$$

    here, $\alpha_i \neq 0$ because $t$ is a unit.

(d) Any rep $\mathbb{Z} \to GL(V)$ with $1 \to g$ can be contained in $k[t, t^{-1}]$. What is the action of $\mathbb{Z} \circlearrowright k[t, t^{-1}]$? well $1 \cdot t^k = t^{k+1}$, so we can think of this as $\ell_{\mathbb{Z}}$, i.e. all bi-infinite sequences where 1 is the right shift action

(e) We now have the map

$$\mathbb{Z} \to \mathbb{Z}/n \implies k[t, t^{-1}] \twoheadrightarrow k[t]/(t^n - 1)$$

what reps of $\mathbb{Z}$ become reps of $\mathbb{Z}/n\mathbb{Z}$? Clearly not $k[t, t^{-1}]$ because that's too large and $t^n \neq 1$. However $k[t, t^{-1}]/(t - \zeta_n^d)^j$ should work where $\zeta_n$ is an $n$th primitive root of unity. Actually, we need $j = 1$, because $(t - \zeta_n^d)^j \mid (t^n - 1)$. By the way, assume that we're in characteristic not dividing $n$

(f) This tells us that any finite dimensional rep of $\mathbb{Z}/n\mathbb{Z}$ over $k = \overline{k}$ with $char(k) \nmid n$ is a direct sum of one dimension irreducibles of the form $k[t, t^{-1}]/(t - \zeta_n^d)$.

(g) When $k$ is not algebraically closed, the irreducibles are $k[t, t^{-1}]/\Phi_k(x)$, where $\Phi_k(x)$ is a cyclotomic polynomial appearing in the factorization of $t^n - 1$

(h) E.g $k = \mathbb{Q}$, $n = 4$, then

$$t^4 - 1 = (t - 1)(t + 1)(t^2 + 1)$$

(i) Now lets look at the group $\mathbb{Z}/p\mathbb{Z}$ (i.e. $n = p$) and $p = char(k)$. Then we're looking at modules over $k[t]/(t^p - 1)$. But now

$$t^p - 1 = (t - 1)^p$$

And so the representations of $\mathbb{Z}/p\mathbb{Z}$ over this field are direct sums of modules of the form

$$k[t]/(t - 1)^k \qquad 1 \leq k \leq p$$

the simple modules occur when $k = 1$

(j) With this technique, we can classify representations of $\mathbb{Z}/n\mathbb{Z}$ for any $n$ over fields of any characteristic

(k) How about $\mathbb{Z} \times \mathbb{Z}$ when $k = \overline{k}$ characteristic 0, then the group algebra is isomorphic to $k[x, y, x^{-1}, y^{-1}]$ and maps $\rho : \mathbb{Z} \times \mathbb{Z} \to GL(V)$ reflects data of $\rho(0, 1)$ and $\rho(1, 0)$ which must be two commuting matrices. What is $mSpeck[x, y, x^{-1}, y^{-1}]$? THinking of this as $k[x, y]_{\{x^k, y^j\}}$, then maximal ideals are still of the form $(x - \alpha, y - \beta)$ where $\alpha, \beta \in k^\times$, and so

$$(1, 0) \to \alpha \cdot Id, \qquad (0, 1) \to \beta \cdot Id$$

(l) On Monday we'll be able to understand all finitely generated representations of all finite abelian groups

(m) Let's finish with an interesting representation

$$k[t]/(t^2 - 1) \leftrightarrow \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = t$$

and

$$k[x, y]/((x - 1)^2, (y - 1)^2) \leftrightarrow M$$

where the basis for the above is $\{1, x, y, xy\}$ and we can determine the matrices by seeing what multiplication by $x$ and $y$ does to this basis. Because $x$ and $y$ commute in the polynomial ring, the corresponding matrices will also commute

# 3/2/20

1. No class until Monday of next week (March 9)

2. Last Time

   (a) We had the motivating example of $S_3$ and the corresponding group ring

   (b) $\mathbb{C}[S_3]$ has center containing $1 = [e]$, $s = [(1\ 2)] + [(2\ 3)] + [(1\ 3)]$, and $t = [(1\ 2\ 3)] + [(1\ 3\ 2)]$

   (c) The multplication table for the center is

$$\left(\begin{array}{c|cccc} & 1 & s & t & \\ \hline 1 & & 1 & s & t \\ s & s & 3 + 3t & 2s & \\ t & & t & 2s & 2 + t \end{array}\right)$$

(d) The group algebra of the center is then

$$\mathbb{C}[s,t]/(t^2-t-2, s^2-3-3t, st-2s)$$

which has maximal ideals of $(s,t)=(\pm 3,2)$ and $(s,t)=(0,1)$

(e) Consider a function which is 0 on two of the three points, and 1 on the last point, we have

$$\frac{-2t+4}{6}, \frac{-s=t+1}{6}, \frac{s+t+1}{6}$$

these are our idempotents because they add up to 1. Moreover, we can translate them directly into elements of the group algebra

$$\frac{-s+t+1}{6} \to \frac{1}{6}\left[e-(1\ 2)-(2\ 3)-(3\ 1)+(1\ 2\ 3)+(1\ 3\ 2)\right]$$
$$\frac{s+t+1}{6} \to \frac{1}{6}\left[e+(1\ 2)+(2\ 3)+(3\ 1)+(1\ 2\ 3)+(1\ 3\ 2)\right]$$
$$\frac{-2t+4}{6} \to \frac{1}{6}\left[4e-2(1\ 2\ 3)-2(1\ 2\ 3)\right]$$

These correspond to the alternating, trivial, and standard representation. Moreover, these correspond to the points in the spectrum: $(-3,2)$, $(3,2)$, and $(0,-1)$, i.e. the points at which those functions do not vanish

(f) Taking a step back, we had

$$\rho : G \to GL(V)$$

a faithful group homomorphism

(g) The degree of the representation is the dimension of $V$

(h) We could construct new representations by taking duals, direct sums, determinants, tensors

(i) $k[G]$ is the group ring, and representations correspond to left modules

(j) THe goal is to classify all finite dimensional $k[G]$-modules

3. Last time, we went over simple modules, irreducible modules, and decomposable modules

4. A module being simple implies that it is indecomposable

5. Completely reducible modules are those which are direct sums of irreducible modules

6. A module is semisimple if it is completely reducible

7. Two modules are isotopic if they decompose into the same direct sum of simple modules

8. Remark: If $V$ is irreducible, then so is $V^*$

9. Dream: All $G$-reps over $k$ are semisimple, with finitely many simples. This is true for vector spaces

10. For modules over groups, we often consider $\mathbb{Z}$-modules and $\mathbb{C}[t]$-modules, but these are not always semisimple unfortunately

11. Rep Theory of finite abelian groups

(a) **Theorem:** For $G=\mathbb{Z}/p\mathbb{Z}$, and $char(k)\neq p$, $k=\overline{k}$ (only need that $t^p-1$ factors completely in $k$),$k[G]=k[t]/(t^p-1)=\prod_{i=1}^{p}k[t]/(t-\zeta^i)$ then the irreps are 1-dimensional and semisimple

(b) The spec looks like the $p$-gon of roots

(c) Idempotents will look like

$$\pi_1 = \frac{1+t+\cdots=t^{p-1}}{p} = \frac{1}{|G|}([0]+[1]+\cdots+[p-1])$$
$$\pi_\zeta = \frac{1}{|G|}([0]+\zeta^{-1}[1]+\zeta^{-2}[2]+\cdots+\zeta^{-(p-1)}[p-1])$$

and any $k[G]$-module, $M$, will be

$$M=\sum_{i=1}^{p}\pi_{\zeta_p^i}M$$

(d) Now note that $\text{Hom}_k(V, W)$ is a $G$-rep, and $\text{Hom}_G(V, W)$ is a vector space. The latter is the collection of all $G$-linear homomorphisms. The action of $G$ on $\phi$ is composition by the inverse, i.e. $\rho : G \to GL(V)$ induces a map $\rho^* : G \to GL(V^*)$ and

$$\rho^*(g) = \rho(g^{-1})^T$$

12. Nonabelian groups

(a) Consider the 1-dimensional representations, we then have $\rho : G \to GL_1(k)$, i.e. $G \mapsto k^\times$ where $k^\times$ is abelian.

(b) In particular $G = G/[G, G] \to k^\times$, i.e. the map factors through the quotient by the commutator.

(c) **Proposition:** Any finite subgroup of $k^\times$ is cyclic

(d) Then one-dimension representations correspond to cyclic quotients of $G$

(e) **Lemma:** (Schur's) If $M$, $N$ simple $R$-modules, then any map $M \to N$ is either any isomorphism or the 0 map.
**Proof:** Consider the kernel and image as submodules of $M$ and $N$ respectively

(f) **Lemma:** (Schur's alternate version) If $M$ is an irrep over $k = \overline{k}$, then $\text{Hom}_k(M, M) = k^\times$.
**Proof:** Consider $\phi : M \to M$. Let $\lambda$ be an eigenvector for some $\phi(g)$, and

$$(\phi - \lambda Id) \in \text{Hom}_k(M, M)$$

with a kernel, meaning that it must be the zero map, and hence $\phi = \lambda Id$ on all of $M$

(g) Consequence: Under the same hypothesis, $\text{Hom}_k(M^n, M^m)$ is the collection of $n \times m$ matrices

(h) **Theorem:** (Maschke's) If $G$ is a finite group and $char(k) \nmid |G|$, given $U \hookrightarrow V$ a subrep, then $\exists W$ such that $U \oplus W = V$ and $W$ is a subrep as well. Equivalently,

$$0 \longrightarrow U \longrightarrow V \longrightarrow W \longrightarrow 0$$

is short exact and splits.
**Proof:** Consider $\pi \in \text{Hom}(V, V)$ such that $\pi : V \to U$ with $\pi\Big|_U = Id$, then

$$\frac{1}{|G|} \sum_{g \in G} [g] \pi \circ g^{-1}$$

is now a map of representations $V \to V$ with $U \xrightarrow{Id} U$. Let $\ker(\pi) = W$. □

(i) **Corollary:** In char 0, every finite dimensional $G$ rep is finite semisimple with the projectors = idempotents

(j) Note:

$$\text{Hom}_{k[G]}(k[G], M) = M$$

If $M$ is irreducible, then $M$ appears in $M$ appears in $k[G]$ with multiple dimension equaling $dim M$

(k) Ex: $S_4$, then we have two 1-dimensional reps, leaving us with 22 dimensions remaining, which is probably $9 + 9 + 4 = 3^2 + 3^2 + 2^2$.

# 3/4/20

No class due to Ravi being out of town

# 3/6/20

No class due to Ravi being out of town

## 3/9/20

1. Today, we are meeting over zoom
2. Ravi wants to finish representation theory
3. Character Theory
   (a) We're working with a finite dimensional representation over an algebraically closed field, i.e. $\rho : G \to GL(V)$ for $|G| < \infty$ and $V$ is a $k$-vector space with $char(k) \nmid |G|$

   (b) If this is an irreducible representation and non-trivial, then

   $$\sum_{g \in G} \rho(g) = 0$$

   this is because if we;re able to divide by the group, then the above (divided by $|G|$) is the projection onto the trivial representation

   (c) Given $\rho$, we can define the character

   $$\chi(\rho) : G \to k \;\text{ s.t. }\; g \mapsto tr(\rho(g))$$

   (d) The trace of the matrix and powers of the matrix encode all of the data of the eigenvalues

   (e) We can also encode the trace via elements of the group algebra

   $$\chi \mapsto \sum_g \chi(\rho)(g)\ [g]$$

   as an example, for the trivial representation, we have

   $$\chi(\rho_{triv}) \mapsto \sum_g [g]$$

   (f) For the regular representation, we get

   $$\chi(\rho_{reg}) = |G|\ [e]$$

   (g) For the permutation representation, we get

   $$\chi(\rho_{perm}) = \sum_g \text{number of fixed points by g } [g]$$

   (h) Other useful facts,

   $$\chi_\rho(e) = \dim\ V$$

   (i) Key property of trace is that it is invariant under conjugation

   (j) $\chi_\rho$ is then a class function, i.e. it's an element of $Z(k[G])$

   (k) The number of copies of the trivial representation in $\rho$ is equal to

   $$\frac{1}{|G|} \sum_{g \in G} \chi_\rho(g)$$

4. Linear Algebra
   (a) A few properties of characters

   $$\chi_{V \oplus W} = \chi_V + \chi_W, \qquad \chi_{V \otimes W}(g) = \chi_V(g)\chi_W(g)$$

   (b) Because of this, the character gives us a map from the ring of representations to $Z(k[G])$

   (c) Here, we can think of the ring of representations as induced by multiplication (tensoring) and summing (direct product) with the trivial representation being the multiplicative identity and the zero representation being the additive identity

(d) This map is a little tricky though because tensoring on the representation side yields convolution as multiplication on the group algebra side

5. Let's look at a $\mathbb{Z}/2\mathbb{Z}$ representation, then we can have multiplication in the group ring of

$$(a[e]+b[i])(c[e]+d[i]) = (ac+bd)[e] + (ad+bc)[i] \neq ac[e]+bd[i]$$

so we really need to do convolution and not just blind multiplication of coefficients for the same group element

6. Characters give a map from $k[G]$ left modules to functions on the conjugacy classes of $G$

7. We have the following results

$$\chi(Sym^2(V)) = \frac{\chi(\rho)^2+\chi(\rho^2)}{2}$$
$$\chi(\wedge^2(V)) = \frac{\chi(\rho)^2-\chi(\rho^2)}{2}$$
$$\chi(\mathrm{Hom}(V,W)) = \chi(V^*\otimes W) = \chi(V^*)\chi(W)$$

8. If $V$, $W$ are irreps then

$$\frac{1}{|G|}\sum_{g\in G}\chi_{V^*}(g)\chi_W(g) = \begin{cases} 1 & V=W \\ 0 & V\neq W \end{cases}$$

and this follows by Schur's lemma

9. **Theorem:**

   (a) We can check if a representation is irreducible

   (b) Character determines the representation

   (c) The number of irreducible representations is less than or equal to the number of conjugacy classes

10. As an example, the conjugacy classes in $S_5$ is a collection of unordered tuples of positive integers which add to 5. The number of these limits the number of the irreducible representations

11. Observation, note that for $k=\mathbb{C}$,

$$\chi(V^*) = \overline{\chi(V)}$$

can we get such a nice relation when $k$ is some other field

12. In particular, the above is true because an eigenvalue for $(\rho, V)$ is some root of unity $\zeta$, and this gives a corresponding eigenvalue for $V^*$, which will be $\zeta^{-1}=\overline{\zeta}$.

13. This gives us a hermitian inner product on representations

$$\frac{1}{|G|}\sum_{g\in G}\overline{\chi_V(g)}\chi_V(g)$$

14. **Theorem:** (over $k=\mathbb{C}$) the number of irreducible representations equals the number of conjugacy classes
**Proof:** Every irreducible representation occurs in the regular representation of $\mathbb{C}[G]$, so it suffices to the count the dimension of each irrep in the regular representation. This will be the dimension of the irrep itself. □

15. Over non-complex fields, the pairing between vector spaces and its dual via this inner product doesn't go through, and so we don't get equality.

16. Ex: Irreps of $S_4$

    (a) Suffices to find the class functions

$$1=[e], \qquad a=\sum i<j[(i\ j)], \qquad b=\sum_{\text{all 3 cycles}}(i\ j\ k), \qquad c=\sum(i\ j\ k\ l) \qquad d=\sum(i\ j)(k\ l)$$

The number of elements in each summand is 1, 6, 8, 3, and 6

(b) From here, we want to find $Spec(Z(\mathbb{C}[S_4]))$ which will determine the irreducible representations, but we can do this because we know how to multiply things

(c) e.g. What is $c^2$? It is some combination of even permutations, and so

$$c^2 = x_0 + x_1 b + x_2 c$$

and in actuality $x_0 = 3$, $x_1 = 0$, $x_2 = 2$, and so we get a quadratic equation

$$c^2 = 2c + 3 \implies c = -1,\ 3$$

(d) Similarly

$$bc = 3b + 0 \cdot c \implies b(c-3) = 0 \implies (b,c) = (0,-1) \text{ or } (b,3)$$

(e) What about $ac$? We should get 18 terms total and they should all be odd (odd times even is odd), so we get

$$ac = xa + yd$$

$a$ and $d$ each consist of 6 terms, so we have $0 \leq x, y \leq 3$, and the right combination will be

$$ac = a + 2d$$

Thus, $c = -1, 3$ gives $a = d$ or $a = -d$, meaning that

$$(a,b,c,d) = (a,0,-1,-a) \text{ or } (a,b,3,a)$$

(f) Finally, let's look at $ab$, which will consist of odd terms, and in particular

$$ab = 4a + 4d$$

If $a = d$, then we get

$$a(b-8) = 0 \implies b = 8$$

If $a = -d$, then $ab = 0$, meaning that we get one of the following three cases in total

$$(a,0,-1,a),\ (0,b,3,0)\ (0,8,3,a)$$

(g) In the end, the five solutions to $(a,b,c,d)$ will give us projectors onto irreps

$$\begin{pmatrix} a & b & c & d \\ 0 & -4 & 3 & 0 \\ 2 & 0 & -1 & -2 \\ -2 & 0 & -1 & 2 \\ 6 & 8 & 3 & 6 \\ -6 & 8 & 3 & 6 \end{pmatrix}$$

the identity/trivial representation corresponds to $(6,8,3,6)$. This is not a complete table, as we need the value of 1, which corresponds to the dimension. Using the condition that the sum of the character values yield 0, we have

$$\begin{pmatrix} 1 & a & b & c & d \\ 1 & 0 & -4 & 3 & 0 \\ 1 & 2 & 0 & -1 & -2 \\ 1 & -2 & 0 & -1 & 2 \\ 1 & 6 & 8 & 3 & 6 \\ 1 & -6 & 8 & 3 & 6 \end{pmatrix}$$

these are not the characters of the irreps, because not all irreps are one dimensional. But after taking an appropriate scaling, we do get them

17. In general, how do we find irreps? Brute force, from nature (looking at $S_4$ as a symmetry group on some object), etc.

# 3/11/20

No class because Ravi got caught up in some logistics. We will have class on Friday, 9:30am - 10:20am.

# 3/13/20

1. 210 B Course Summary
2. Ravi has a hand out and is going pretty fast, so I'll let the reader refer to his notes
3. Galois Theory
    (a) One hard fact from Galois theory: If we have $G \circlearrowright E$ for $E$ a field, then

    $$\begin{tikzcd} E \arrow[d, dash, "|G|"] \\ E^G \end{tikzcd}$$

    where $E^G$ is the fixed field of $G$. This comes from the linear independence of characters
4. Commutative Algebra
    (a) Understand rings through their ideals and modules
    (b) Understand Hilbert's Nullstellensatz, and Zariski's lemma
    (c) See problem 21 from the homeworks
5. Finite extension theory
    (a) In a UFD, codimension 1 prime ideals are principal
    (b) Zariski's lemma was proved via dimension theory, and somehow dimension theory is the right setting for it
6. Rep theory
    (a) Fundamental idea is $Spec(Z(k[G])) =$ collection of all irreducible representations