MATH 210B NOTES

ARUN DEBRAY
DECEMBER 22, 2014

CONTENTS

Part 1. Galois Theory

1. ALGEBRAIC EXTENSIONS AND SPLITTING FIELDS: 1/6/14

Any map between fields $i : k \to L$ is injective, because the kernel must be an ideal of k, so it's either $\{0\}$ or k, and all ring maps must preserve the identity,[1] so it cannot be the zero map. (All rings in this class will be associative, commutative, and with 1, and all ring maps must send $1 \mapsto 1$; useful examples exist when any of these requirements are relaxed, but not for this class.)

[1]Note that Dummit & Foote do not adhere to this convention.

Example 1.1. There are two maps $\mathbf{Q}[\sqrt{3}] \rightrightarrows \mathbf{R}$: one sends $a + b\sqrt{3} \mapsto a + b\sqrt{3}$ and the other sends $a + b\sqrt{3} \mapsto a - b\sqrt{3}$.

Typically, once the injection is specified, the notation is suppressed into $k \subseteq L$.

Definition.

- An extension of a field k is a pair (L, i) (more often written L or L/k, the latter where there is no ambiguity over quotients), where $i : k \to L$ is a field map.
- Given two extensions $L_1, L_2/k$, a map $L_1 \to L_2$ as extensions (also, "over k") is a map that makes the following diagram commute.

$$\begin{tikzcd} L_1 \arrow[rr] & & L_2 \\ & k \arrow[ul, "i_1"] \arrow[ur, "i_2"'] & \end{tikzcd}$$

In other words, a map of field extensions has to respect how k is embedded in L_1. One could think of $k \subseteq L_1 \subseteq L_2$, which is more useful in practice, but the proofs are often easier when one uses maps.[2]

Definition. Given an extension L/k, an $a \in L$ is algebraic over k if there exists a nonzero $f \in k[X]$ such that $f(a) = 0$. The whole extension L/k is algebraic if all $a \in L$ are algebraic over k.

This definition takes a somewhat implicit step: f can be regarded as an element of $L[X]$ because $i : k \to L$ induces a map $k[X] \to L[X]$. Also, by suitable $k^\times$-scaling, one can always arrange for f to be monic. This is a pretty common state of affairs.

Given an algebraic $a \in L$ over k, there is an evaluation map, called evaluation at a: $\mathrm{ev}_a : k[X] \to L$ given by $x \mapsto a$ and thus $f \mapsto f(a)$. Notice that the kernel is nonzero, so it must be a principal ideal: $\ker(\mathrm{ev}_a) = (f_a)$ for some monic $f \in k[X]$ with positive degree (since we're not in Dummit-and-Foote-land, so $1 \not\mapsto 0$). Thus, one obtains the following isomorphism: $k[X]/(f_a) \xrightarrow{\sim} k[a]$. Since $k[a] \subseteq L$ and a subring of a field must be a domain, then $k[a]$ is a domain, and therefore (f_a) is prime and f_a is irreducible.

Definition. The above polynomial f_a is called the minimal polynomial of a.

For $f \in k[X]$ irreducible, (f) is easily seen to be a maximal ideal, so $k[X]/(f)$ is always a field, which has k-dimension (as a vector space; the dimension of L over k is denoted $[L : k]$) $\deg(f)$. Thus, the above $k[a]$ is a field, and $[k[a] : k] = \deg(f_a)$. Thus, $k[a] = k(a)$, i.e. its fraction field, since it's a field.

However, a finite-degree extension L/k need *not* be of the form $k(a)$ (though this is the case in characteristic zero); an example is given in the homework. This is OK; sometimes, one can prove things by reducing the problem to a tower of primitive extensions (i.e. those generated by a single element), though not always.

There's a standard construction that turns all of this around: given some irreducible $f \in k[X]$ (which can be chosen to be monic), there exists a field $K := k[X]/(f)$. letting $a = X \bmod f$, $f(a) = 0$. This is abstract, and the advantage of such an abstract construction is that if one has two extensions L_1 and L_2 of k, then they are unrelated abstract extensions, so it's a lot easier to handle the maps between them.

Claim. For example, suppose $L_1, L_2/k$ are such that $a_1 \in L_1$ and $a_2 \in L_2$ are both roots of an irreducible $f \in k[X]$. Then, $k(a_1) \cong k(a_2)$ over k, and the isomorphism sends $a_1 \mapsto a_2$.

Proof. If such an isomorphism exists, it is clearly unique, because $a_1 \mapsto a_2$ forces the whole map.

As for existence: one has $k[X]/(f) \xrightarrow{\sim} k[a_2] = k(a_2)$ that sends $X \mapsto a_2$, and similarly for a_1 and $k(a_1)$, so take the first isomorphism and compose it with the inverse of the second to obtain an isomorphism sending $a_1 \mapsto a_2$ between $k(a_1)$ and $k(a_2)$. ⊠

Thus, one can speak of "the" extension given by a root of an irreducible polynomial, because all such extentions are isomorphic. Observe that the proof made use of the abstract construction, which is less messy than the alternative.

Warning: notation such as $\mathbf{Q}(\sqrt[3]{2})$ is ambiguous, because there are three such roots, and in some contexts using the real or complex roots could have different outcomes. Algebraically and abstractly, they're the same, but in $\mathbf{C}$ they aren't. Thus, it's more common to write $\mathbf{Q}(\alpha)$ where $\alpha^3 = 2$. This is more clearly abstract.

[2] A brief historical note on the roots (heh) of Galois theory: the original formulation focused on the zeros of polynomials, and explicit calculation of permutations. The newer, more abstract approach involving field extensions is much easier, and due to Artin and Noether at the head of the 20^{th} Century.

On the subject of abstractness, it's *really, really bad* to ask whether two extensions are equal; it's nearly meaningless. The more useful question is whether they're isomorphic over the ground field. This signals that one must choose the isomorphism, which is important; otherwise, there could be confusion and mistakes because two people chose different isomorphisms. Inside some ambient field, yes, one can speak of strict equality, but in general two isomorphisms differ by an automorphism, and automorphisms of field extensions is only the whole point of Galois theory.

More generally, given a nonconstant $f \in k[X]$ (which can be made to be monic, again), one can build a finite extension K/k such that in $K[X]$, $f(X) = c \cdot \prod(X - r_i)$, for some $c \in K^\times$ and $r_i \in K$. Since $K[X]$ is a UFD, then such a collection $\{r_i\}$ with multiplicity is of course uniquely determined if it exists. A procedure for constructing such a field is as follows: first, choose some irreducible factor $\pi \mid f$ in $k[X]$, and then define $K_1 = k[X]/(\pi)$ and $a_1 = X \bmod \pi$. Then, in $K_1[X]$, $f(X) = (X - a_1)f_1(X)$ with $\deg(f_1) < \deg(f)$, so it's possible to keep going, However, f_1 isn't necessarily irreducible, so sometimes one has $K = k$. However, in all cases one must have $[K : k] \le n!$, where $\deg(f) = n$, since the maximum degree of extension i is $\deg(f_i)$.

Though... how would we know whether the result of this process is unique? Or rather, if one has two such extensions, are they isomorphic?

Definition. A splitting field L/k of a monic, nonconstant $f \in k[X]$ is an extension such that

(1) $f = c \cdot \prod(X - r_i)$ in $L[X]$, with $c \in L^\times$.
(2) The more important part: $L = k[r_1, \dots, r_n]$.

A splitting field is like Goldilocks and the n Bears: big enough to contain all of the roots of f, but not too big — it contains nothing more.[3]

Splitting fields exist by the above construction. The uniqueness result illustrates why the abstract viewpoint is so much better.

Proposition 1.1. *Given a field k and a monic, non-constant $f \in k[X]$,*

(1) Any two splitting fields $L_1, L_2/k$ of f are isomorphic.
(2) If f splits completely in L/k, then there is a unique subfied F of L containing k that is a splitting field.

Proof. For (2), it's forced, because $F = k[r_1, \dots, r_n]$, where $f = \prod(X - r_i)$ in $L[X]$.

(1) requires a little more cleverness. Specifically, induct on $\deg(f)$, but over all possible ground fields k.

Choose an irreducible factor $\pi \mid f$ in $k[X]$, and let $a_i \in L_i$ be a root of π (i.e. $a_1 \in L_1$ and $a_2 \in L_2$ are both roots). These exist because π splits completely in $L_i[X]$. Then, let $K = k[T]/(\pi)$ and $a = T \bmod \pi$, soth at $f(X) = (X - a)g(X)$ in $K[X]$, where $\deg(g) < \deg(f)$. Then:

$$\begin{tikzcd}
L_1 \supseteq k(a_1) \arrow[r, "\sim", "a_1 \mapsto a"'] \arrow[dr, dash] & K & k(a_2) \subseteq L_2 \arrow[l, "\sim"', "a \leftarrow a_2"] \arrow[dl, dash] \\
& k &
\end{tikzcd}$$

Now, by composing the maps $K \xrightarrow{\sim} k(a_1) \hookrightarrow L_1$, L_1 is realized as a splitting field of g over K. But so is L_2, and $\deg(g) < \deg(f)$, so one can apply induction. Then, the K-isomorphism given by induction is also a k-isomorphism, because everything commutes in the following diagram:

$$\begin{tikzcd}
L_1 \arrow[rr, "\sim"] \arrow[dr, dash] \arrow[ddr, dash, bend right] & & L_2 \arrow[dl, dash] \arrow[ddl, dash, bend left] \\
& K \arrow[d, dash] & \\
& k &
\end{tikzcd}$$

⊠

For the next couple of weeks, this will be used over and over. Notice the trick of leaving the ground field unspecified; it's important, since it would be a lot messier otherwise. It's also important that f isn't necessarily irreducible, because even if one starts with an irreducible f, there's no guarantee that the resulting g is reducible. The idea is that the hypothesis had to be relaxed to make the induction stronger. However, if one chooses f to be irreducible, there's a nice corrolary:

Corollary 1.2. *If $f \in k[X]$ is irreducible and $L_1, L_2/k$ are splitting fields of f, then for any $a_1 \in L_1$ and $a_2 \in L_2$ that are roots of f, there exists a k-isomorphism $L_1 \to L_2$ such that $a_1 \mapsto a_2$.*

[3]That $k[r_1, \dots, r_n]$ is a field, and therefore equal to $k(r_1, \dots, r_n)$, is courtesy of Homework 1.

Of course, this is totally wrong when f is reducible.

In particular, if L is a splitting field of f over k, which is sometimes denoted $L = \mathrm{split}_k(f)$, where $f \in k[X]$ is irreducible, then $\mathrm{Aut}(L/k)$ acts transitively on the set of roots of f in L. This will be useful later.

It's also possible to talk about the field extension which splits all polynomials over a given field, but actually constructing such a field is a bit tricky: since these extensions are all abstract, it's hard to speak about their unions and intersections. Thankfully, there's a good way to handle this: tune in Wednesday to bring some closure to this story.

2. Algebraic Closure and Zorn's Lemma: 1/8/14

The basic point that ensures algebraicity is well-defined is a bit of trivial linear algebra, but its generalization to rings will be extremely useful later in the course. This is: if L/k and $a \in L$, then a is algebraic over k if $k[a] \subset L$ is finite-dimensional as a k-vector space. The proof involves linear independence, or a lack of it, in that a. a^2, etc. satisfy some relations. The same idea will be applied to ring etensions, but requires integrality and lots of other exciting stuff.

This gives a couple nice consequences: for example, if $a, b \in L$ are algebraic over k, then $k[a, b] \subset L$ is a finite-dimensional k-algebra, so $k[a \pm b]$ and $k[ab]$ are finite-dimensional over k (since they're subspaces of $k[a, b]$), and thus $a \pm b$ and ab are also algebraic over k. Likewise, $1/a$ is algebraic if $a \neq 0$.

The point is, the algebraic elements of L form a field.

Definition. The subfield $k' = \{a \in L \mid a \text{ is algebraic over } k\} \subseteq L$ is called the algebraic closure of k in L.

Exercise 2.1. If $L = k(X)$, the field of rational functions in one variable, show that $k' = k$. Hint: first, go from $k(x)$ to $k[x]$, much like the rational root theorem for $\mathbf{Z} \subset \mathbf{Q}\ldots$ then, being algebraic is equivalent to satsifying a monic relation, and one can just talk about $k[X]$ and invoke degree.

Example 2.1. This construction is actually meaningful: if $k = \mathbf{Q}$ and $L = \mathbf{C}$, then $k' = \overline{\mathbf{Q}}$, the algebraic numbers in $\mathbf{C}$.

By its very definition, k' is an algebraic extension of k, though it's not necessarily finite. But its name also suggests that it should be maximal, and it does indeed have a transitivity relation.

Lemma 2.1. *If k —— F —— L is a tower, then L/F and F/k are algebraic iff L/k is algebraic.*

Corollary 2.2. $(k')' = k'$*, i.e. k' contains all other algebraic exensions of k in L.*

Proof of Lemma 2.1. In the reverse direction, suppose that L is algebraic over k. Then, L is clearly algebraic over F, because any $a \in L$ satisfies the same monic relations over F as over k, and $F \subseteq L$, so everything in F is algebraic over k as well.

In the more interesting direction, choose a $c \in L$. Then, $f(c) = 0$ for some monic $f = \sum a_i X^i \in F[X]$. Now, the coefficients a_i are algebraic over k. Though we recently saw that the sum and product of algebraic elements are again algebraic, we don't yet have an explicit formula for them. Fortunately, this computation can be avoided. Consider $k[a_0, \ldots, a_{n-1}, c] \subseteq L$. This is a finite-dimensional k-subalgebra, because each of the a_i and c are finite-dimensional over k, and thus $k[c]$ is finite-dimensional over k, which means that c is algebraic over k. ⊠

Example 2.2. Once again consider $\mathbf{C}/\mathbf{Q}$ and $\overline{\mathbf{Q}}$. Notice that $\overline{\mathbf{Q}}$ is countable, because there are only countably many monic polynomials in $\mathbf{Q}[X]$. But it has the nice property that it is algebraically closed in its own right.

Lemma 2.3. *Suppose that k is a field. Then, the following are equivalent:*

1. *All nonconstant polynomials over k have a root.*
2. *All irreducibles in $k[X]$ have degree 1.*
3. *k has no nontrivial finite extensions.*
4. *k has no nontrivial algebraic extensions.*

If these hold, then k is said to be algebraically closed.

Proof. First, (1) $\iff$ (2) just by thinking about unique factorization. Morever, (3) $\iff$ (4): if L/k is a finite extension, then clearly it's algebraic, and if L/k is algebraic, then for any $a \in L$, $k[a]/k$ is finite.

To show (3) implies (2), suppose $f \in k[X]$ is irreducible of degree d. Then, $k[X]/(f)$ is a finite extension of k, of degree d. The reverse direction is similar. ⊠

In the spirit of Goldilocks and the Three Bears, one wants a field extension that is just big enough not to have any nontrival algebraic extensions, but just small enough to be algebraic. Can this always be done for a given k? Historically, all of this was done embedded within $\mathbf{C}$, which made answering these questions a little less interesting.

Claim. If L/k, L is algebraically closed, and k' is the algebraic closure of k in L, then k' is algebraically closed. In particular, $\overline{\mathbf{Q}}$ is algebraically closed.

Proof. Suppose K' has a finite extensions K/k' such that $K \neq k'$. Choose an $a \in K \setminus k'$, which has a minimal polynomial $f \in k'[X]$ of degree greater than 1. Thus, we have $K \supset k'[a] \cong k'[X]/(f)$.

Since $L \supset k'$ and is algebraically closed, choose a root $r \in L$ of f, since one can view f as in $L[X]$, but then $r \in L$ is algebraic over k', and thus $r \in k'$. But r is a root of the irreducible f of degree greater than 1, which is a contradiction. ⊠

This is nice: L can be as huge as I want, but now, given one algebraically closed extension, there must be an algebraic one. However, there are some questions still: is it unique, or does it depends on the choice of k'? Also, does such a field L necessarily exist? Historically, again, $\mathbf{C}$ was the solution, but in characteristic p or for the p-adics this doesn't exactly work.

Definition. An algebraic closure of k is an algebraic extension $\overline{k}/k$ such that $\overline{k}$ is algebraically closed.

From above, one already has the example $\overline{\mathbf{Q}}/\mathbf{Q}$. Now, the questions posed beforehand can be reformulated: if $\overline{k}$ and $\overline{k}'$ are algebraic closures of k, is there a k-isomorphism between them? This is sort of the infinite analogue of the uniqueness of splitting fields; the algebraic closure is in some sense a splitting field of everything. More worryingly, does such a $\overline{k}$ even exist?

If k is countable, e.g. $\mathbf{Q}$, then $k[X]$ is countable, so each minimal polynomial can be enumerated and then split one at a time, giving a recursive process. of course, this doesn't work for uncountable fields. $\mathbf{R}$ in $\mathbf{C}$ isn't too tricky, but what about $\mathbf{R}(X)$? The study of irreducibles in $\mathbf{C}(X)$ is the entire theory of compact Riemann surfaces! In general, having an algebraic closure is useful, especially with regards to these sorts of questions about algebraic curves.

First, we address uniqueness. Often, when trying to prove existence in algebra or geometry, proving uniqueness is helpful, since it adds structure, making it a better approach. However, the proof here is too floppy to be helpful.

Proposition 2.4. *Suppose K_1 and K_2 are algebraic closures of k. Then, $K_1 \xrightarrow{\sim} K_2$ over k.*

Notice that this isomorphism isn't special; there are lots of them, so it's not a good idea to say that $K_1 = K_2$.

Proof of Proposition 2.4. As a warm-up, if $k \subseteq F \subseteq K_1$ such that F is a finite extension, then F can be put inside K_2 by expressing it as a tower of primitive extensions $k(a_1)$, $k(a_1, a_2)$, and so on, or in several other ways. Then, pick a minimal polynomial for a_1, which provides a root in K_2, and so one can embed $k(a_1)$ in K_2, and so on. But this doesn't work for K_1 as a whole, which isn't finite, and so one must use... Zorn's lemma.

Anytime you need to do a 'big' construction and the finite case is noce, then Zorn's lemma is pretty useful.

Consider pairs (F, i), where $k \subset F \subset K_1$ and $i : F \to K_2$, where F isn't necessarily finite. Then, say that $(F', i') \geq (F, i)$ if $F' \supseteq F$ and i, i' are compatible, in that the following diagram commutes:

$$\begin{tikzcd} F' \arrow[rr, "i'"] & & K \\ & F \arrow[ul] \arrow[ur, "i"'] & \end{tikzcd}$$

Let $\Sigma = \{(F, i)\}$; with this $\geq$, Σ is a partially ordered set since not all elements are comparable: notice that if $F' \geq F$ and $F' \leq F$, then $F' = F$; this is stronger than isomorphism, since it can be taken within the ambient field K_1.

Recall that if $(S, \geq)$ is a partially ordered set, then a *chain* in S is a subset $T \subset S$ such that for all $t, t' \in T$, $t \leq t'$ or $t \geq t'$; that is, all elements of T are comparable. In our situation, every chain has an upper bound. If $\{(F_\alpha, i_\alpha)\}$ is a chain in Σ, then $F = \bigcup_\alpha F_\alpha \subset K_1$ is a field, because any two of the F_α are related: one is contained within the other.[4] Moreover, these i_α "glue" to form a map $i : F \to K_2$, and (F, i) becomes an upper bound to the chain.

Zorn's Lemma. *If $(S, \leq)$ is a nonempty partially ordered set with all chains bounded above, then it admits a maximal element.*

Thus, there exists an $F \subset K_1$ with $i : F \to K_2$ a k-map that cannot be nontrivially extended.

Lemma 2.5. $F = K_1$.

Proof. Use the fact that K_1/F is algebraic and K_2/F is algebraically closed to pick an $a \in K_1 \setminus F$, so one can find a root of its minimal polynomial in K_2 and construct $F(a)$ and a map $F(a) \to K_2$ that extends F.

The entire proof of Proposition 2.4 will be finished next lecture, as it remains to be shown that $i : K_1 \to K_2$ is actually an isomorphism.

[4]It is not true in general that $F \cup F'$ is a field, even when F and F' are.

The proof from last lecture of Proposition 2.4 was unfinished. We found a map $j : K_1 \to K_2$, but it remains to show that it is an isomorphism. Since it is a map of field extensions, then it is injective. For surjectivity, pick an $a' \in K_2$, which has a minimal polynomial $f \in k[X]$, since K_2 is algebraic. Then, f splits completely in $K_1[X]$ as $f(X) = \prod(X - r_i)$, where the r_i are (not necessarily distinct) roots. From j one gets a map $K_1[X] \to K_2[X]$ over $k[X]$, so in $K_2[X]$, $f(X) = \prod(X - j(r_i))$. Since $f(a') = 0$ in K', then $0 = \prod(a' - j(r_i))$, so $a' = j(r_i)$ for some i.⊠

Here, the proof depended on on factoring polynomials. Variations of this trick will come up next week. Unlike some proofs of uniqueness, this one doesn't offer a construction.

The proof of existence offered below is a variant of the standard construction which only takes one step, and is otherwise due to Artin. The idea is to take a huge polynomial ring with one variable for each polynomial in $k[X]$ and then mod out by a maximal ideal. This will be slightly different, and is sort of like the Hahn-Banach theorem in that you should see the proof once, but after that can use the result all the time without worry. In general, life becomes really nice by extending to an algebraic closure.

Thus, introduce

$$A = k\left[t_{f,j} \mid \begin{array}{l} f \in k[X] \text{ is monic and irreducible} \\ 1 \le j \le \deg(f) \end{array} \right].$$ [5]

For any $f \in A[X]$, one can write

$$f(X) - \prod_{j=1}^{\deg(f)} (X - t_{f,j}) = \sum_{i=0}^{\deg(f)} c_i(f) X^i,$$

for some c_i corresponding to symmetric functions and signs whose exact natures are unimportant. Then, let $J = (c_i(f))_{f, 0 \le i \le \deg(f)} \subset A$. This ends up being a maximal ideal, yielding a field that is algebraic and in which everything splits completely.

Claim. $J \ne (1)$ in A.

Proof. Suppose $1 \in J$. The fact that J is made of finite linear combinations of elements makes life easier.[6] In particular, the way that $1 \in J$ is expressed using only finitely many $t_{f,j}$, so 1 actually lies in $A_0 = k[t_{\alpha,j} \mid 1 \le j \le \deg(f_\alpha)]$ for some $\{f_1, \dots, f_n\}$.

Let $K = \mathrm{split}_k(f_1, \dots, f_n)$, so that in $K[X]$, one can write

$$f_\alpha(X) = \prod_{j=1}^{\deg(f_\alpha)} (X - r_{j,\alpha}).$$

One common way to show something doesn't hold is to make a map to something else that is (non)zero, so construct a map $A_0 \to K$ by sending $t_{f_\alpha,j} \mapsto r_{j,\alpha}$,[7] which is a k-algebra map. Thus, in the induced map $A_0[X] \to K[X]$, $f_\alpha(X)$ and $\prod(X - t_{f_\alpha,j})$ both map to $f_\alpha(X) = \prod(x - r_{j,\alpha})$, so their difference goes to zero, and $c_0(f_\alpha), c_1(f_\alpha), \dots \mapsto 0$ in K. Thus, they couldn't have generated 1 in A_0. Oops. ⊠

The trick used in the above claim is much like the idea that one can check if something isn't a unit in a ring by sending it to another, more tangible ring and checking if the result is a unit there.

Proposition 3.1. *If R is a commutative ring and $I \subsetneq R$ is a proper ideal, then there exists a maximal ideal M of R containing I.*

The proof of this proposition uses Zorn's lemma, and it will be briefly deferred. Notice that the proof breaks down if R is not commutative, which says some interesting things about division algebras.

Assuming Proposition 3.1, pick a maximal ideal M of A such that $J \subseteq M \subset A$, and let $F = A/M \supset k$. In $F[X]$, every monic monic irreducible $f \in k[X]$ splits completely, since $M \supseteq J$; this field is rigged to make that happen. Moreover, by design, F is generated as a k-algebra by those roots, so F/k is algebraic.

Claim. Since F/k is algebraic and every monic irreducible in $k[X]$ splits completely in $F[X]$, then F is algebraically closed.

[5] Don't worry about the distinctness of the roots of f; if one tries to localize to ensure the roots are all distinct, the end result is the zero ring, which is unhelpful to say the least.

[6] This is much like doing things over $\mathbf{Q}$ in which one only actually needs $\mathbf{Z}[1/n_1, \dots, 1/n_k]$, which sometimes helps. In this regard it also resembles proofs of quasi-compactness in algebra, where the same finiteness trick is used.

[7] In order to make this map, one needs to enumerate the roots $r_{i,\alpha}$, but since there are a finite number of them, this is perfectly OK.

Proof. Suppose $F/'F$ is an algebraic extension, so that one wants to show that $F' = F$. Since F/k is also algebraic, then by transitivity of algebraicity, F' is also algebraic over k, so every $a \in F'$ has some minimal polynomial $f \in k[X]$. But in $F[X]$, f splits as $f(X) = \prod(X - r_i)$, and in F', $0 = f(a) = \prod(a - r_i)$, so $a = r_i$ for some i, an d therefore $a \in F$. ⊠

Thus, the construction of an algebraic closure is complete, conditioned on the existence of that maximal ideal.[8]

Proof of Proposition 3.1. Pass to R/I; then, it suffices to show that every nonzero commutative ring has a maximal ideal (since a maximal ideal of R/I has preimage in R and contains I).

Apply Zorn's lemma to the collection of proper ideals of R, ordered by inclusion: $I \geq J$ iff $I \supseteq J$. Then, every chain is bounded above, because one can take its union, though it requires some effort to show that this union is proper (which follows because $I \neq R$ iff $1 \notin I$). Thus, by Zorn's lemma, there exists a maximal ideal. ⊠

So it's worth pointing out that the above proof breaks down in the case of an associative, non-commutative ring. But where? It turns out the issue is finding a divion algebra quotient. With Zorn's lemma, one can show that every two-sided ideal is contained within a maximal two-sided ideal, but constructing two-sided ideals in non-commutative rings is hard.[9]

Definition. An algebraic extension L/k is normal if every irreducible $f \in k[X]$ with a root in L splits (i.e. splits completely) over L.

Claim. If L is a splitting field over k of some non-constant (not necessarily irreducible) $F \in k[X]$, then L/k is normal.

Proof. The proof uses the crutch of an algebraic closure. Maybe it's blowing things out of proportion, but it makes life easier, and provides another illustration of the utility of seeing field extensios as inclusions. As an exercise, it's possible to rework this proof without the algebraic closure, instead building the common extension in another way.

Pick an irreducible $f \in k[X]$ with a root $a \in L$, and the goal is to show that f splits over L, and let $K = \text{split}_k(f) = k(a_1, \dots, a_n)$, where these a_i are the roots of f. Specifically, pick an algebraic closure $\overline{k}$ of k, and construct K within $\overline{k}$. Then, $L \supset k(a)$ is finite over k, and the goal is to stuff it into $\overline{k}$ and show that it actually ends up in K.

Choose a map $L \hookrightarrow \overline{k}$, because $\overline{k}$ must contan a splitting field of f, L is also a splitting field, and any such two fields are abstractly isomorphic. Since a is a root of f, then this inclusion must carry a to a root of f: $a \mapsto a_{i_0}$ for some a_{i_0}. But automorphisms of a splitting field move any root of f to any other root; specifically, for any i, there exists a $\sigma \in \text{Aut}_k(K)$ such that $\sigma(a_{i_0}) = a_i$. Thus, $\overline{k}$ is realized as an algebraic closure in two ways: through the embedding j made at the beginning, and $\sigma \circ j$. Thus, there is an isomorphism $\widetilde{\sigma} : \overline{k} \to \overline{k}$ (by uniqueness of an algebraic closure) sending $a_{i_0} \mapsto a_i$.

Then, look at $\widetilde{\sigma} : L \hookrightarrow \overline{k}$ over k. This moves $a \mapsto a_i$, but since L is a splitting field, then any automorphism must send it back to itself: $\widetilde{\sigma}(L) = L$. Thus, $a_i \in L$ for every i, and thus $K \subseteq L$ inside $\overline{k}$. ⊠

[8] This is not the usual proof, which adds the roots one at a time. Thus, if you ever see it in a textbook, please let me or Professor Conrad know; it would be useful as a reference.

[9] To give a bit more perspective on the fact that it is hard to find quotients of non-commutative associative rings that are division algebras, consider these facts (sent to the students in an email):

1. Matrix algebras $\text{Mat}_n(k)$ over a field are the ur-example of a "simple ring." It has no nonzero proper 2-sided ideals, and for $n > 1$ is not a division algebra. In view of the Artin-Wedderburn theorem (see Wikipedia...), it is very ubiquitous among finite-dimensional associative algebras over a field for there to be no division algebra quotient.
2. Division algebras finite-dimensional over a field are useful! For instance, this comes up when one is confronted with understanding finite group representations over fields that are not alg. closed. Indeed, if G is a finite group and $\rho : G \to \text{GL}(V)$ is a finite-dimensional irreducible representation over a field k then $\text{End}_{k[G]}(V)$ is a finite-dimensional division algebra over k (well, its center might be a finite extension of k), and if k is not algebraically closed then this is generally non-commutative. So there's nothing at all like Schur's Lemma in such situations, and one has to grapple with division algebras over k in classifying such representations.
   Going further with this second point, it transpires that knowing the structure of division algebras finite-dimensional over a field is a key ingredient to answer natural questions like the following (which are perfectly interesting even over ground fields such as $\mathbf{R}$ and $\mathbf{Q}$ and $\mathbf{F}_p$): if K/k is a finite extension and an irreducible K-linear representation ρ of G has all $g \in G$ acting with characteristic polynomial lying in $k[X]$ (not just in $K[X]$) then does ρ descend to a linear representation over k? The answer turns out to always be affirmative over finite fields due to special features of Galois theory over finite fields, but it can fail over $\mathbf{R}$ and is a very subtle number-theoretic problem over $\mathbf{Q}$ (getting involved with local-global principles in number theory).

Note: the first five minutes of today's lecture were given by Professor Venkatesh, covering because Professor Conrad was running slightly late.

Recall that L/k is a normal extension if for every irreducible $f \in k[X]$ which has a root in L splits in L. An important non-example is to let α be a root of X^3-2. Then, in $\mathbf{Q}(\alpha)$, $X^3-2 = X^3-\alpha^3 = (X-\alpha)(X^2+\alpha X+\alpha^2)$, but this has discriminant $-3\alpha^2$, which is not a square in L because there exists an embedding $L \hookrightarrow \mathbf{R}$ (in general, it's more useful to view these as abstract objects, but this illustrates why it doesn't work). Thus, L is not normal.

A better way to think about normality than the definition (whose actual proof will be given in just a bit) is that when a normal extension is embedded in the algebraic closure, its image is always the same, even if the maps themselves differ. This related to Galois-theoretic properties of normality.

Normality is a strong property, so it would be nice to have some actual examples.

Proposition 4.1. *If L/k is a finite extension of fields, then it is normal iff $L = \operatorname{split}_k(f)$ (i.e. it is* a *splitting field) for some nonconstant $f \in k[X]$.*

Proof. The reverse direction was given last time, so for the forward direction, assume that L/k is normal. Then, choose a k-basis $\{a_1,\dots,a_n\}$ of L, and let m_{a_i} be the minimal polynomial for a_i over k (since each of these extensions is finite, then it's algebraic, so I can do this), so m_{a_i} splits over L by normality. Thus, L is the splitting field of $f = \prod M_{a_i}$. ⊠

In this case, f isn't irreducible. Can a different f' be chosen in general to be irreducible? In other words, is every normal extension the splitting field of an irreducible polynomial?

Next, some elementary properties of normality are given.

Definition. If $\{L_\alpha\}$ is a set of field extensions of k embedded in some ambient field L, then the compositum of all of the L_α is the field generated by finite linear combinations of elements of the L_α over k. Observe that the choice of embedding into L can affect the result of this operation.

Theorem 4.2.

1. *If L/k is an algebraic extension, then L is normal iff it is the compositum of finite normal sub-extensions L_α/k.*
2. *If $k \subseteq k' \subseteq L$ and L/k is normal, then L/k' is normal.*[10]

Proof. For (1), in the forward direction: the goal is to show that every element of L lies in a finite normal subextension. Choose some $a \in L$; then, $m_a \in k[X]$ splits over L, so $a \in \operatorname{split}_k(m_a) \subset L$ over k, but by Proposition 4.1, this is finite and normal over k.

In the reverse direction, given some finite normal subextensions $\{L_\alpha\}$ in L/k with L their compositum, suppose $f \in k[X]$ is irreducible with a root $a \in L$. Then, we want f to split completely. Since L is made of finite combinations of elements from the $\{L_\alpha\}$, then $a \in L_{\alpha_1}\cdots L_{\alpha_n}$, i.e. some finite compositum over k. But we already know that $L_{\alpha_1} = \operatorname{split}_k(f_i) \subseteq L$ for some nonconstant $f_i \in k[X]$, so $L_{\alpha_1}\cdots L_{\alpha_n} = \operatorname{split}_k\left(\prod f_i\right) \subseteq L$ (since all of the roots lie in the finite compositum), and thus f splits over this subextension of L over k, so it splits in L. ⊠

All the real content in this proof was in a previous lecture: that the splitting field of a polynomial is normal.

Theorem 4.3. *For an algebraic extension L/k, L is normal iff all k-embeddings $L \overset{j}{\hookrightarrow} \overline{k}$ have the same image $j(L)$ inside k.*

Proof. The intuition at the finite level is that splitting fields must go to themselves in algebraic closures, because endomorphisms send roots to each other.

In the forwrd direction, pick a normal extension L/k, which by the previous theorem implies that it's a compositum of finite normal subextensions $\{L_\alpha\}$. Thus, $j(L)$ is the compositum over k of all of the $j(L_\alpha)$, so it's enough to treat the case of the L_α, i.e. one can assume L is finite.

Then, L is the splitting field of some $f \in k[X]$, so $j(L)$ is a splitting field of f in $\overline{k}$, which is independent of the choice of j, because it is generated by the roots of f within $\overline{k}$. Thus, $j(L)$ is always the same.

In the reverse direction, one uses automorphisms of $\overline{k}$ to move roots of f around.[11] Choose an irreducible $f \in k[X]$ with a root $a \in L$. Thus, it's enough to show that f splits completely in $j(L)$, since this would force it to

[10] Note that k'/k is in general not normal, e.g. $k = \mathbf{Q}$, $k' = \mathbf{Q}(\sqrt[3]{2})$, and L is a splitting field of X^3-2.

[11] Aside: if for psychological reasons one wanted to reduce to the finite case here, too, it's perfectly possible, by showing that k-embeddings into $\overline{k}$ of intermediate extensions of L/k extend to embeddings $L \hookrightarrow \overline{k}$ over k, but it's not necessary to do so.

also split in L. By hypothesis, $j(L)$ is independent of j, so it must be closed under automorphisms of $\overline{k}$, because a $\sigma \in \mathrm{Aut}_k(\overline{k})$ induces another inclusion $j' = \sigma \circ j$.

Since $\overline{k}$ is algebraically closed, f splits over it. Thus, for any root $b \in \overline{k}$ of f, it's enough to show that $b \in j(L)$. But $j(a) \in j(L)$ is a root of f, so there is an isomorphism $k(j(a)) \xrightarrow{\sim} k(b)$ over k. This must extend into $\overline{k}$, since $\overline{k}$ is unique,[12] so there is an automorphism $\sigma : \overline{k} \xrightarrow{\sim} \overline{k}$ sending $j(a) \mapsto b$. Thus, $b \in j(L)$. ⊠

This is the best way to think of normal extensions, that the copy inside the algebraic closure is well-defined, even as the way it's put in might change. Though "most" extensions aren't normal, one can make a similar construction for a field, embedding it in a smallest normal extension. That is, for an irreducible $f \in k[X]$, we already have $k(a)$ and $\mathrm{split}_k(f)$, both unique up to isomorphism. But the goal is to speak of $\mathrm{split}_k(f)$ in terms of a $j : k(a) \hookrightarrow \mathrm{split}_k(f)$ over k without explicitly referring to f. This notion is known as the normal closure.

Definition. If L/k is algebraic, a normal closure is an algebraic extension L'/L such that:

(1) L'/k is normal, and
(2) for any normal F/k and $L \overset{j}{\hookrightarrow} F$, there exists a $j' : L' \hookrightarrow F$ over L.

Example 4.1. If $L = k[X]/(f)$ for an irreducible f, then $L' = \mathrm{split}_k(L)$ once a root of f in L is chosen (so that L' is realized over L, not just over k). This is because the lifting property allows one to embed L into the splitting field once this root is chosen. It works because we have enough automorphisms of splitting fields.

A much less interesting example is that of a normal extension: if L/k is normal, then $L' = L$.

Theorem 4.4. *Let L/k be algebraic. Then,*

(1) there exists a normal closure for L, and
(2) if L_1' and L_2' are normal closures of L, then $L_1' \xrightarrow{\sim} L_2'$ over L.

Proof. For (1), work in an algebraic closure $\overline{k}$ of k, and choose an $L \hookrightarrow \overline{k}$ that fixes k. Then, let L' be the compositum in $\overline{k}$ of $\mathrm{split}_k(m_a) \subset \overline{k}$ for every $a \in L$. This is a normal extension, because it's a compositum of finite normal extensions, so suppose that F/L is an extension that's normal over k. Then, an algebraic closure $\overline{F}$ of F must be isomorphic to $\overline{k}$, since it's also an algebraic closure for k, so the resulting embedding $\tilde{j} : F \hookrightarrow \overline{k}$ is compatible with the induced $j : L \hookrightarrow \overline{k}$. By normality, since F/k is normal and $\tilde{j}(F) \supset j(L)$, then the image must contain L'.

For (2), suppose there exist L_1' and L_2' that are normal closures of some L/k. Thus, there must exist embeddings $L_1' \hookrightarrow L_2'$ and $L_2' \hookrightarrow L_1'$, since they're both minimal normal extensions.

Showing that the composite of these maps is an isomorphism implies that each one is, and furthermore, it's enough to show that for any algebraic K/k, any embedding $K \hookrightarrow K$ must be an isomorphism.[13] This is because for every $a \in K$, j carries the set of roots of m_a in K into itself, and therefore onto itself (since it's a finite set), so some other root in K is the preimage of a. ⊠

5. More Normality and Separability: 1/15/14

Today's lecture was started by Daniel Litt, in the same way, for the same reasons, and for the same length of time as last lecture.

Theorem 5.1. *Suppose $k \subseteq k' \subseteq L$, where L/k is a normal, algebraic extension and L/k' is normal. Then, k'/k is normal iff for all $\sigma \in \mathrm{Aut}(L/k)$, $\sigma(k') = k'$ iff for all $\sigma \in \mathrm{Aut}(L/k)$, $\sigma(k') \subseteq k'$. Moreover, in such cases, the restriction map $\mathrm{Aut}(L/k) \to \mathrm{Aut}(k'/k)$ given by $\sigma \mapsto \sigma|_k$ is surjective.*

Remark. The last equivalence follows because an endomorphism of an algebraic extension is necessarily an isomorphism. Algebraicity is necessary, because over $\mathbf{Q}$, $\mathbf{Q}(t) \to \mathbf{Q}(t)$ given by $t \mapsto t^2$ is otherwise a counterexample.

Exercise 5.1. Suppose $f \in \mathbf{Q}[t]$ is a polynomial with no repeated roots. Then, show that in $\mathbf{Q}(t)(\sqrt{f(t)})$, such an endomorphism exists if $\deg(f) = 3$ or 4, but not if it's larger. Hint: this has something to do with elliptic curves.

Another example in positive characteristic is $K \to K$ given by $a \mapsto a^p$. This is not the identity on very many subfields.

Remark. If one has an intermediate extension that isn't normal, the automorphisms can detect that, though it's not super useful. For example, take $L = \mathbf{Q}(\sqrt[3]{2}, \zeta_3)$ and $k = \mathbf{Q}$, so that $L = \mathrm{split}_{\mathbf{Q}}(x^3 - 2)$. If $k' = \mathbf{Q}(\sqrt[3]{2})$, then k'/k is not normal, which implies there are automorphisms of L/k that don't preserve k'.

[12] What's going on here is that $\overline{k}$ is realized as two algebraic closures of $k(j(a))$: through the embedding implicitly chosen at the start of the proof when we said "work in an algebraic closure" and that map composed with this isomorphism.
[13] This is trivial for finite extensions, and for nromal extensions can be exhausted by splitting fields.

Proof of Theorem 5.1. In the forward direction, we know k' is a compositum over k inside L of some *finite* normal subextensions $k_\alpha = \mathrm{split}_k(f_\alpha)$ for $f_\alpha \in k[X]$. Then, $\sigma(k')$ is the compositum over k inside L of $\sigma(k_\alpha) = k_\alpha$, since $\sigma(f_\alpha) = f_\alpha$. Thus, $\sigma(k') = k'$ again.

In the reverse directio, the content is the characterization of normality inside the algebraic closure. Thus, work in an algebraic closure $\overline{k}$. The other useful fact in this proof (which remains to be proven) is that every algebraic extension F/k admits a k-embedding j into $\overline{k}$, and that $\mathrm{Aut}(\overline{k}/k)$ acts transitively on the set of such embeddings (i.e. any one is carried to any other by some automorphism).

One of many ways to prove this is to pick an algebraic closure $\overline{F}$ of F, so that $\overline{F}$ is also an algebraic closure of k, so $\overline{F} \xrightarrow{\sim} \overline{k}$ over k, and restricting to F gives an embedding. So an embedding exists.

Suppose that one has two embeddings $j, j' : F \hookrightarrow \overline{k}$. These both realize $\overline{k}$ as an algebraic closure of F in two ways, so there is an isomoprhism $\sigma : \overline{k} \xrightarrow{\sim} \overline{k}$ carrying j to j' over F: $\sigma \circ j = j'$. Then, since j and j' are over k, one can check that this σ also fixes k.

Now, assuming that $\mathrm{Aut}(L/k)$ preserves k', we want to show that k'/k is normal. Well, choose $L \hookrightarrow \overline{k}$ ove k. By normality, this is stable under $\mathrm{Aut}(\overline{k}/k)$, but by the fact just shown, the resulting restriction[14] map $\mathrm{Aut}(\overline{k}/k) \to \mathrm{Aut}(L/k)$ is surjective, because for any automorphism of L realizes $\overline{k}$ as an algebraic closure of L in two ways, yielding an isomorphism $\sigma : \overline{k} \to \overline{k}$. Thus, $k' \hookrightarrow \overline{k}$ as a subfield is preserved under all $\sigma \in \mathrm{Aut}(\overline{k}/k)$.

Once again, we can prove the normality using the criterion from last lecture, so suppose there exist maps $j_1, j_2 k' \rightrightarrows \overline{k}$ are two k-embeddings. Then, since there must be a $\sigma \in \mathrm{Aut}(\overline{k}/k)$ such that $\sigma \circ j_1 = j_2$, then $\sigma(j_1(k')) = j_2(k')$, and therefore $j_1(k') = j_2(k')$. ⊠

The most important point is that a normal extension always has the same image inside the algebraic closure. This is really just doing some group theory behind the scenes, of course, as a normal subgroup is just such that $gHg^{-1} = H$ or $gHg^{-1} \subseteq H$ (since applying g^{-1} shows these conditions are equivalent) for all $g \in G$. THs is the metaphor or analogue.

However, as in group theory, a normal subgroup of a normal subgroup isn't normal, and the same thing is going on here. There's something similar going on in the definition of solvable, nilpotent, etc. groups, those given by a composition series: the definitions can be made surprisingly restricted, yet end up equivalent.

However, normality of field extensions is *not* transitive. For example, take $\mathbf{Q} \overset{2}{\text{——}} \mathbf{Q}(\sqrt{2}) \overset{2}{\text{——}} \mathbf{Q}(\sqrt[4]{2})$; $x^4 - 2$ has roots over $\mathbf{Q}(\sqrt[4]{2})$, yet doesn't split completely.

Moving forward, the next topic is separability, which scares people until they get used to it. Be careful: some textbooks do this wrong, e.g. developing Galois theory only over characteristic 0 or such to avoid it.

Definition. A nonzero $f \in k[X]$ is separable if it has $d = \deg(f)$ distinct roots in a splitting field over k.

By the uniqueness of splitting fields, this is a well-defined notion.

Example 5.1. If $k = \mathbf{Q}$, then $f(X) = X^n - 1$ is separable, because its roots in $\mathbf{C}$ are the vertices of the regular n-gon, $\{\zeta^j\}_{0 \le j < n}$, where $\zeta = e^{2\pi i/n}$.

Another example in characteristic p is $X^p - X - a$, which appears in the homework.

For a non-example, suppose $f = h^2 g$ where $\deg(h) > 1$. This isn't terribly interesting, compared to an irreducible example: suppose $\mathrm{char}(k) > 0$ and $a \in k \setminus k^p$ (i.e., a is not a p^{th} power, implying that k cannot be a finite field). Then, as will be shown in the homework, $T^{p^r} - a \in k[T]$ is irreducible, and if α is a root of this polynomial in an extension of k, then $(T-\alpha)^{p^r} = T^{p^r} - \alpha^{p^r} = T^{p^r} - a$. A specific example is $k = \mathbf{F}_p(X)$ and $a = X$.

The essential case is the irreducible case, so we can reduce[15] to that case. For a monic $f \in k[X]$, f is separable iff $f = \prod f_i$, where the f_i are distinct, monic irreducibles over k that are irreducible.

Claim. If $f_1, f_2 \in k[X]$ are distinct monic irreducibles, then they cannot share a root in an extension field of k.

Proof. By monicity and irreducibility, $\gcd(f_1, f_2) = 1$. Thus, there exist $h_1, h_2 \in k[X]$ such that $f_1 h_1 + f_2 h_2 = 1$. This is inherited over every extension, so there can't be a common root, because plugging it in implies that $0 = 1$. ⊠

How can one detect separability over k without leaving k? We use calculus! One can define the notion of a derivative $\frac{\mathrm{d}}{\mathrm{d}X} : k[X] \to k[X]$ purely algebraically, with the usual operations, though a slicker idea is to work in $k[X, H] = k[X][H]$, defining $f(X + H) = f_0(X) + f_1(X)H + f_2(X)H^2 + \cdots$, where $f_i(X)$ is its i^{th} derivative. Thus, one can actually prove the Leibniz rule rather than assuming it.

---

[14] To even have a well-posed restriction map requires the image in the algebraic closure to be uniquely determined, which requires normality.

[15] No pun intended.

Theorem 5.2. *For nonzero $f \in k[X]$, f is separable iff* $\gcd(f, f') = 1$.

The crux of the argument is that the gcd doesn't change over extensions, so one can calculate over the extension field.

6. More Separability: 1/17/14

Daniel Litt started today's lecture again, and went for about five minutes.

Last time, we saw the differential criterion for separability, that $f \in k[X]$ is separable iff $\gcd(f, f') = 1$, proven in a handout.[16] If you've only seen Galois theory over characteristic 0, this could be a new thing.

Definition. A commutative ring is reduced if it has no nonzero nilpotents.

For example, $\mathbf{Z}/15$ is reduced, but $\mathbf{Z}/75$ isn't, because $15^2 \equiv 0 \bmod 75$.

Another criterion for separability, via the k-algebra $A = k[X]/(f)$, is more useful for rings later on. This states that f is separable iff $A \otimes_k k'$ is reduced for all k'/k. This will be a homework exercise; it's not rocket science. But this tensorial criterion makes sense in a much wider context than just field extensions.

Today we will discuss how far a general polynomial is from a separable polynomial, especially if f is irreducible.

Proposition 6.1. *For an irreducible $f \in k[X]$, f is not separable iff $f' = 0$ iff* $\mathrm{char}(k) = p > 0$ *and $f = g(X^p)$ for a irreducible $g \in k[X]$.*

Proof. Without loss of generality, assume that f is monic, so $\gcd(f, f') = 1$ or f. But $\deg(f') < \deg(f)$, so if f isn't separable, then $\gcd(f, f') = f$, and therefore $f \mid f'$. This forces $f' = 0$. Since $\deg(f) > 0$, then the only way for its derivative to vanish is for every x^i in f has $i = 0$ in k, i.e. k has positive characteristic. Thus, $p \mid i$ for all i, so $f = g(X^p)$. Clearly, g must be irreducible, or else it factors, so f does as well. ⊠

Note that a given irreducible $g \in k[X]$ in characteristic p doesn't always yield an irreducible $g(X^p) = f$, e.g. $g(X) = X$. In practice, this ends up being not so important. Note also that in the above setup, $f = g(X^p)$, and if g is not separable, then $g = h(X^p)$, so $f = h(X^{p^2})$, and so on. In the end, $f = F(X^{p^e})$ for some $e \geq 0$, where F is a separable irreducible in $k[X]$. F is sometimes called the separable part of f, denoted f_{sep}.

Corollary 6.2. *For an irreducible $f \in k[X]$, f is separable if* $\mathrm{char}(k) = 0$*, and if* $\mathrm{char}(k) = p > 0$*, then $f = f_{\mathrm{sep}}(X^{p^e})$, where f_{sep} is given above.*

Let's look at the second case more closely: we want facts about polynomials to make sense for field extensions. Thus, consider the extension $k(a)/k$, where $f(a) = 0$, and inside of it, $k(b)$, where $b = a^{p^e}$. Then, $f_{\mathrm{sep}}(b) = 0$, and in $k(a)/k(b)$, $T^{p^e} - b$ vanishes at a. Since b isn't a p^{th} power in $k(b)$, then this polynomial in $k(b)[T]$ is irreducible.

Though this looks as if it depends strongly on the choice of a, it will be seen that parceling out a separable piece and an inseparable piece works for general field extensions in positive characteristic. Then, most proofs split into two pieces: the separable part is treated with Galois theory, and the inseparable part is handled separately, since all of the extensions are given by p^{th}-power roots. This concrete construction is pretty fortituous.

Remark. Over a splitting field of f, $f = \prod (x - r_i)^{p^e}$ for pairwise distinct roots $\{r_i^{p^e}\}$ of f_{sep}. In particular, for any root a of f, a^{p^e} is separable over k.

Definition. Sometimes, people want to unite these discissions, so they use a notion called the characteristic exponent of k, which is 1 if $\mathrm{char}(k) = 0$ and is p if $\mathrm{char}(k) = p > 0$.

A guy named Ritt inroduced differental Galois theory to understand which ODEs or integrals can be solved in terms of certain nice functions. This all happened over characteristic 0.

Definition. For an algebraic extension L/k, an $a \in L$ is separable over k if its minimal polynomial $f \in k[X]$ is separable. L/k is separable if every $a \in L$ is separable.

Of course, both of these notions are automatic in characteristic 0.

This is an *a priori* strong assumption, but like normality we will eventually discover that if $a \in L$ is separable over k, then $k(a)/k$ is separable. There are two proofs of this idea: the classical notion counts embeddings, but there's a much slicker way of using the tensorial criterion.[17] The former uses yet another criterion that L is separable if there exist $[L : k]$ embeddings $L \hookrightarrow \overline{k}$.

[16] This differential criterion is reminiscent of the Implicit Function theorem, in which all of the zeros of f and f' don't vanish. This is no coincidence: it has vast algebraic-geometric consequences in several variables.

[17] The tensorial criterion is akin to (because of deep voodoo scheme-theoretic generalizations) the statement that if there are local isomorphisms of manifolds $M \cong N$ and $N \cong P$, then $M \cong P$ locally as well.

Definition. A field k is perfect if all of its algebraic extensions are separable. Equivalently (which you can check), every irreducible polynomial is separable.

Lemma 6.3.

1. *If* $\mathrm{char}(k) = 0$*, then k is perfect; if* $\mathrm{char}(k) = p$*, then k is perfect iff $k = k^p$, i.e. every element in k is a p^{th} power.*
2. *All finite fields are perfect.*
3. *If k is perfect, then so is every algebraic extension of k, in particular algebraic extensions of $\mathbf{F}_p$.*

This seems to eliminate a lot of options! But there are still interesting and useful imperfect fields, such as $\mathbf{F}_p(X)$ within algebraic number theory.

Proof of Lemma 6.3. For part (1), this is obvious for characteristic zero. For characteristic p, if there exists an $a \in k \setminus k^p$, then $T^p - a \in k[T]$ is irreducible, but it only has one root in $\overline{k}$, showing k is not perfect. If instead everything in k is a p^{th} power, then pick an irreducible $f \in k[X]$; if f is not separable, then $f = g(X^p)$ for $g(X) = b_n X^n + \cdots + b_0 \in k[X]$, so $b_i = c_i^p$, so $g(X) = \sum c_i^p X^{pi} = \left(\sum c_i X^i\right)^p$, which is a problem, because f is supposed to be irreducible.

For (2), if k is finite, then $c \mapsto c^p$ is an injective ring homomorphism, hence surjective. Then, apply (1).

For (3), suppose L/k is algebraic and k is perfect. Then, let L'/L be algebraic, so that L'/k is too. Then, every $a \in L$ is separable over k, and therefore its minimal polynomial over k, $f_a \in k[X]$, is separable. But its minimal polynomial g_a over L is a factor of f_a, so it must still be separable.

⊠

Theorem 6.4.

1. *If $k \subseteq k' \subseteq L$ is a tower, then L/k is separable iff L/k' and k'/k are separable.*
2. *If $L = k(a)$ with a separable over k, then L/k is separable.*

Proof. For (1), in the forward direction: any $a \in k'$ viewed in L has the same minimal polynomial over k, so k'/k is separable, and likewise, if $a \in L$, then its minimal polynomial over k' divides its minimal polynomial over k (in $k'[X]$); hence, it is separable. This is the same idea as in the proof of Lemma 6.3, above.

The other direction is tricker, and uses yet another separability criterion. The proof will be given next time.

For item (2), choose a $b \in L = k(a) = k[a]$, and we want f_b, its minimal polynomial, to be separable. There is an injection $B = k[b] \hookrightarrow k[a] = A$. To prove the theorem, the tensorial criterion comes in handy, i.e. $B \otimes_k \overline{k} \hookrightarrow A \otimes_k \overline{k}$ as k-algebras. But $A \otimes_k \overline{k}$ is reduced by the criterion, so its subrings are too. Thus, $B \otimes_k \overline{k}$ is also reduced, and therefore f_b must be separable. ⊠

7. Transitivity of Separability: 1/21/14

Recall that last time, the tensorial criterion for separability was presented: that f_a is separable iff $k(a) \otimes_k \overline{k}$ is reduced, as will be shown on Homework 3. More generally, f is separable iff $(k[X]/(f)) \otimes_k \overline{k}$ is reduced; by universal properties, this is isomorphic to $\overline{k}[X]/(f)$.

Remark. In the separable case,

$$\begin{aligned} k(a) \otimes_k \overline{k} &= (k[X]/(f_a)) \otimes_k \overline{k} \\ &= \overline{k}[X]/\left(\prod_i (x - r_i)\right) \\ &\cong \prod_i \overline{k}[X]/(x - r_i) \cong \prod_i \overline{k}, \end{aligned}$$

by the Chinese Remainder theorem. However, this is as k-algebras; when keeping track of the ring structure, it's more important to preserve it.

The actual isomorphism can be written down: suppose $\sigma : k(a) \to \overline{k}$ is an embedding over k, and let Σ be the set of such embeddings. Then, the isomorphism

$$k(a) \otimes_k \overline{k} \xrightarrow{\sim} \prod_{\sigma \in \Sigma} \overline{k}$$

is described by sending $a \otimes 1 \mapsto (\sigma(a))_{\sigma \in \Sigma}$.

Describing this k-algebra as copies of $\overline{k}$ allows one to feed this tensorial criterion of separability into itself, in order to prove transitivity of separability for field extensions. The rough idea is that if L/k' and k'/k are finite and separable, then $L \otimes_k \overline{k} \cong L \otimes_{k'} (k' \otimes_k k)$ as rings. Then, breaking the inside apart leads to the proof, but there are nuances about the extension not necessarily being primitive. The proof as a whole is slicker, but more exotic.

Today, though, we'll prove transitivity of separability by the counting criterion, yet another criterion dealing with field embeddings into an algebraic closure.

Proposition 7.1. $\#\operatorname{Hom}_k(k(b), \overline{k}) \leq \deg(f_b) = [k(b) : k]$, *with equality iff b is separable over k.*

Proof. A map $k(b) = k[X]/(f_b) \to \overline{k}$ must send b to a root of f_b in $\overline{k}$, so there are at most $\deg(f_b)$ choices, and there are $\deg(f_b)$ choices iff f_b has exactly that many roots, i.e. b is separable. ⊠

Of course, this is really the same thing as the tensorial proof, where we're implicitly constructing the equivalence $\operatorname{Hom}_k(A, \overline{k}) = \operatorname{Hom}_{k\text{-Alg}}(A \otimes_k \overline{k}, \overline{k})$. In any case, this proposition will be stated and proven in greater generality later on.

Here is a useful application.

Proposition 7.2. *$k(a)/k$ is separable if f_a is separable over k.*

Proof. Choose a $b \in k(a)$, so that we want f_b to be separable over k. Then, without loss of generality, $\operatorname{char}(k) = p > 0$ (or else we're done), so $f_b = (f_b)_{\text{sep}}(X^{p^e})$ where $(f_b)_{\text{sep}}$ is separable and irreducible, and $e \geq 0$. Thus,

$$\begin{tikzcd}
k \arrow[r, dash, "d_3"] \arrow[rr, dash, bend right, "\deg(f_b)"'] \arrow[rrr, dash, bend right=60, "d_1 d_2 d_3"'] & k(b^{p^e}) \arrow[r, dash, "d_2"] & k(b) \arrow[r, dash, "d_1"] & k(a)
\end{tikzcd}$$

Here, $d_3 = \deg((f_b)_{\text{sep}})$. Now, we want to show that $\#\operatorname{Hom}_k(k(a), k) = d_1 d_2 d_3$, but let's calculate it in another way. Since $(f_b)_{\text{sep}}$ is separable, then $\#\operatorname{Hom}_k(k(b^{p^e}), \overline{k}) = d_3$, but there is exctly one way to lift this to $k(b)$. This is the miracle of characteristic p; the p^{th} root is unique. Next, there are at most d_1 lifts to $k(a)$ (in fact, exactly d_1 such lifts, because it divides the minimal polynomial for a over k), and so there must be at most $d_1 d_3$ such lifts. We also know there are $d_1 d_2 d_3$ of them, so $d_2 = 1$. ⊠

Now, how robust is the notion of separability? If L/K' and k'/k are separable, then is the whole thing separable? This can be proven using the tensorial criterion and the associativity of tensor products, but it's a little trickier, so we'll use the counting criterion again. But we need a more general form of it first.

Theorem 7.3. *Let L/k be a finite extension and L'/L be a normal extension (e.g. an algebraic closure), and assume there exists an $L \hookrightarrow L'$ over k. Then, $\#\operatorname{Hom}_k(L, L') \leq [L : k]$, with equality iff f is separable.*

Note that L is not *a priori* assumed to be a primitive extention. Also, one often lazily takes $L' = \overline{k}$.

Proof of Theorem 7.3. The proof will be by induction on the number of generators, first for the inequality, then for the equality. Write $L = k(a_1, \dots, a_n)$; If $n = 1$, then it's immediate by the normality of L'/k.

More generally, $L = k(a_1)(a_2, \dots, a_n)$. Then,

$$\#\operatorname{Hom}_k(L, L') = \sum_{\sigma : k(a_1) \hookrightarrow L' \text{ over } k} \# \left\{ \begin{tikzcd}[column sep=small] L \arrow[rr, hook, "?"] & & L' \\ & k(a_1) \arrow[ul, dash] \arrow[ur, dash, "\sigma"'] & \end{tikzcd} \right\}.$$

This makes L' a normal extenion of $k(a_1)$, since L'/k is normal and σ is a k-embedding, by Theorem 4.2. Then, by the inductive step,

$$\begin{aligned} &= \sum_{\leq [k(a_1):k]} [L : k(a_1)] \\ &\leq [k(a_1) : k][L : k(a_1)] = [L : k] \end{aligned}$$

Now, we do another inductive pass. Equality holds iff we have equality at both intermediate stages: $k(a_1)/k$ and $L/k(a_1)$ are both separable. So we can't use the tower argument just yet, but if L/k is separable, then equality holds.

Suppose L/k is not separable, so that there's a $b \in L$ that isn't separable over k. Then, we have the following setup:

$$k \xrightarrow{\quad \deg((f_b)_{\mathrm{sep}}) \quad} k(b^{p^e}) \xrightarrow{\quad <p^e \quad} k(p) \xrightarrow{\quad d_1 \quad} L$$

The first two extensions, though, are primitive, so there's at most one way of lifting $k(b^{p^e}) \hookrightarrow L$ to $k(b)$. Since it's already been proven in general, then there must be at most $d_1 d_3$ embeddings, which is less than $d_1 d_2 d_3 = [L : k]$. ⊠

The proof doesn't seem to use the normality of L' if one doesn't look carefully: it's needed for the base case of the induction.

Like the Fundamental Theorem of Calculus, it's perfectly OK to forget how to prove this; just use the result often.

Theorem 7.4. *If L/k' and k'/k are both separable, then L/k is separable.*

Proof. First, reduce to the finite case, where all the work is.[18] Choose an $a \in L$, so that it satisfies some separable monic $f \in k'[X]$: $f = \sum c_i X^i$ and $f(a) = 0$. Thus, to understand a, we only need these coefficients. Thus, take $K = k(c_1, c_2, \dots)$, so that K/k is finite and separable (since it's inside k'), and $K(a)/K$ is certainly separable, since it has one generator.

Now, pass to $K(a)/K/k$; we can assume these are all finite extensions. We'll count, using k-embeddings into $\overline{k}$ to minimize the amount of thinking we have to do. There are $[k' : k]$ embeddings $k' \hookrightarrow k$, and each of these identifies $\overline{k}$ as an algebraic closure of k, so applying the criterion again, there are $[L : k']$ lifts to L. Thus, the total number of lifts from k to L is $[k' : k][L : k'] = [L : k]$. ⊠

Notice, again, that the whole reason this works is because of the viewpoint of field extensions as maps, rather than inclusions.

Theorem 7.5. *If $\{k_\alpha\}$ are such that $k_\alpha \subseteq K$ and each k_α/k is separable, then their compositum is also separable over k.*

Proof. We can pass to the case of a finite number of k_α, and even $n = 2$ (since the compositum is associative: $k_1 \cdot k_2 \cdots k_n = k_1 \cdot (k_2 \cdot (\cdots k_n) \cdots))$. Thus, the situation now looks like

$$k \xrightarrow{\text{sep.}} k_1 \longrightarrow k_1 k_2,$$

so if we show that $k_1 k_2 / k_1$ is separable, then we're good to go. Since any $x \in k_1 k_2$ involves only finitely many elements of k_2, we can without loss of generality assume that $[k_2 : k]$ is finite; then, express k_2/k as a finite number of primitive extensions, which are all separable because k_2/k is. Then, use transitivity of separability over and over... ⊠

There is also a tensorial proof of transitivity.

Lemma 7.6. *If K/k is finite separable, then $K \otimes_k \overline{k} \cong \overline{k}^n$ as $\overline{k}$-algebras.*

Proof sketch. Write K/k as an iterated tower of primitive extensions and then invoke the associativity of the tensor product.

Now, we can use the lemma: $L \otimes_k \overline{k} = L \otimes_{k'} (k' \otimes_k \overline{k})$, but

$$k' \otimes_k \overline{k} \cong \prod_{\substack{\sigma : k' \hookrightarrow k \\ \text{over } k}} \overline{k}$$

as $\overline{k}$-algebras, and as a k'-algebra, it's inherited by each factor over k. Thus, this is also equal to $\prod (L \otimes_k' \overline{k})$, so it's reduced, and thus separable.

It's the same game, really; if one asks what the meaning of these factors is, it's pretty much identical to the counting argument above, though the tensorial criterion is much nicer.

[18] Why only finite extensions? The answer is that the separable closure of a field is very useful, sort of like the universal cover of a topological space: even though a lot of work is done in the cases of finite coverings, the absolute Galois group is akin to the fundamental group.

8. The Primitive Element Theorem: 1/22/14

Theorem 8.1 (Primitive Element). *If K/k is a finite, separable extension, then it has a primitive element, i.e. $K = k(a)$.*

The converse is often untrure, e.g. if a isn't separable over k.
There's a refinement, which is pretty, but useless.

Theorem 8.2. *A finite extension K/k is primitive iff it has only finitely many intermediate extensions.*

For a proof, see the handout.[19] This is a generalization of Theorem 8.1 because of Galois theory: finite subgroups of finite Galois groups, and so on.

Proof of Theorem 8.1. Write $K = k(a_1, \dots, a_n) = k(a_1, \dots, a_{n-1})(a_n)$. Thus, $k(a_1, \dots, a_{n-1})$ is a subfield, so it's also separable over k. Thus, by induction, the key case is $n = 2$, so assume $K = k(a, b)$ for $a, b \neq 0$.

Now, the goal is to show that $K = k(a + tb)$ for "most" $t \in k^\times$.

For a given $t \in k^\times$, consider $K_t = k(a + tb) \subset K$. We can use the counting criterion to compute the k-degrees. Restriction gives a map $\mathrm{Hom}_k(K, \overline{k}) \twoheadrightarrow \mathrm{Hom}_k)(K_t, \overline{k})$ (which is surjective because any $k_t \hookrightarrow \overline{k}$ can be lifted), but we need it to be injective, i.e. that if $j, j' : k(a, b) \rightrightarrows \overline{k}$ are distinct, then we want $j(a + tb) \neq j'(a + tb)$ for a well-chosen t.

Since j and j' are distinct on $k(a, b)$, then $j(a) \neq j'(a)$ or $j(b) \neq j'(b)$, so without loss of generality assume the latter. Since these are maps over k, then $j(a + tb) = j(a) + tj(b)$, and similarly with j'. If they're equal, then $j(a) - j'(a) = t(j'(b) - j(b))$; since $t \neq 0$ and both sides are nonzero, then since $j(b) \neq j'(b)$, then we can divide: $t = (j(a) - j'(a))/(j'(b) - j(b)) \in \overline{k}$.

However, for varying $j' \neq j$ distinct on b, the possible rations are only finitely many elements of $\overline{k}$, but $t \in k$, so if k is infinite, then one can just choose it to avoid these.

If instead k is finite, then K is finite too, so $K^\times$ is cyclic, so $K^\times = \langle \gamma \rangle$. Then, of course, it's certainly generated by γ.[20] ⊠

Corollary 8.3. *If K/k is finite, separable, and normal, then it's the splitting field of some irreducible $f \in k[X]$.*

This is true because such a K has a primitive element a, and then, by normality, K splits the roots of its minimal polynomial.

Sometimes, a field being the splitting field of a polynomial is not obvious, but in this case it's pretty nice.

Here are two constructions that can be made with separable extensions.

(1) If K/k is a separable extension (maybe not of finite degree), then its normal closure K'/k is also separable, because K' is built inside $\overline{k}$ as the compositum of the splitting fields $F_a = \mathrm{split}_k(f_a)$ for $a \in L$, where f_a is separable and irreducible. Each F_a is separable over k, and hence so is their compositum.

(2) If K/k is a general algebraic extension, there exists a maximal separable subextension F/k, i.e. F/k is separable and it contains all separable subextensions inside K. Specifically, F is the compositum of all separable subextensions, so it contains all of them, and by Theorem 7.5, it too is separable.

In characteristic 0, $F = K$. But in characteristic $p > 0$, any $a \in K$ has $a^{p^e} \in F$, so K/F has nothing separable — just a bunch of p^{th}-power root extractions. These sorts of things (with no natural separable subextensions) are called purely inseparable; though Galois theory can't handle it, such an extension is a perfectly tangible object. Because of the p^{th}-power roots, $\mathrm{Aut}(K/F) = 1$.

Then, F is called the separable closure of k in K. If $K = \overline{k}$, this is *the* separable closure of k, denoted k_s. It's unique up to isomorphism, in the same way and for the same reason that algebraic closures are. Basically, if k_s and k_s' are both separable closures of k, then we get a diagram:

$$\begin{tikzcd}
\overline{k} \arrow[d, no head] & & \overline{k} \arrow[d, no head] \\
k_s \arrow[rr, hook] \arrow[dr, no head] & & k_s' \arrow[dl, no head] \\
& k &
\end{tikzcd}$$

[19] `http://math.stanford.edu/~conrad/210BPage/handouts/insepdegree.pdf`

[20] It's often the case that a theorem in algebra or algebraic geometry requires two proofs, one where the field is infinite and one where the proof is finite. Occasionally, things are false over finite fields, though not this time.

It's really the same idea as that for the algebraic closure.

The idea that the normal closure is separable means that separability is robust. This is useful.[21]

Exercise 8.1. Show that k_s is a separable extension that is its own separable closure.

Definition. A field is separably closed if it has no nontrivial separable extensions.

Over characteristic zero, of course, this is the same thing as algebraically closed.

A nice analogy, far beyond the scope of this course, is that k_s/k is akin to having a "nice" topological space, i.e. one with a fundamental group, and its universal cover. This covering space theory looks very like Galois theory, and Grothendieck introduced the notion of a Galois category to unify these notions.

The General Structure of Finite Extensions. If L/k is finite, then we have k'/k separable and L/k' purely inseparable as above, where k' is the separable closure of k in L. This is a generalization of the case we saw earlier, where k —— $k(a^{p^e})$ —— $k(a)$, but in general one *can't* flip this and place the separable extension on top.[22] This is not a huge problem, but the perspective to keep in mind is that the separable part will always be at the bottom.

In this setup, define the separable degree to be $[L:k]_s = [k':k]$, and the inseparable degree to be $[L:k]_i = [L:k']$. This is a quite tangible notion: $[L:k]_s = \#\operatorname{Hom}_k(k',\overline{k}) = \#\operatorname{Hom}_k(L,\overline{k})$ (since $\operatorname{Aut}(L/k') = 1$ as noted before).

Definition. An algebraic extension is Galois if it is separable and normal.

For example, $\overline{k}/k$ is Galois if k is perfect, and k_s/k is always Galois.

Remark. An algebraic extension K/k is Galois iff K is the compositum of finite Galois subextension k_α/k.

Proof sketch. Choose splitting fields for every minimal polynomial f_α where $\alpha \in K$, and take the compositum of these splitting fields.

Remark. Let $E = \{y^2 = x^3 + 5x - 7\} \cup \{\infty\}$, which is an elliptic curve. This has a commutative algebraic group structure on its points in $\overline{\mathbf{Q}}$ (or in $\mathbf{C}$), which is not obvious — but to study the set of rational points $E(\mathbf{Q})$ one often uses Galois-theoretic information about the kernel of the $(p^k)^{\text{th}}$ power map for some prime p; these turn out to be finite sets of points in $\overline{\mathbf{Q}}$, and these coordinates generate finite Galois extensions over $\mathbf{Q}$, but they have to be assembled into something infinite.

There are lots of similar examples. It's somewhat similar to congruences: one can test whether two numbers are equal, but it's necessary to have an infinite sequence to work with.

We can prove a refinement of the counting lemma.

Lemma 8.4. *For finite extensions L/k, $\#\operatorname{Aut}(L/k) \le [L:k]$, with equality iff L/k is Galois.*

Proof. Fix $L \overset{j}{\hookrightarrow} \overline{k}$ over k. By precomposing j with an automorphism, any automorphism of L gives rise to another embedding, so that $\#\operatorname{Aut}_k(L) \le \operatorname{Hom}_k(L,\overline{k}) \le [L:k]$ (the latter by Theorem 7.3).

Then, equality holds iff both of them are equal, i.e. L/k is separable (for the second half) and L/k is normal (for the first inequality). That is, equality means that any embedding is obtained from precomposing an automorphism of L, so they all must have the same image in $\overline{k}$. ⊠

In general, if K/k is Galois (maybe of infinite degree), we define $\operatorname{Gal}(K/k) = \operatorname{Aut}(K/k)$. For example, if $K = \operatorname{split}_{\mathbf{Q}}(x^3-2)$, then $|\operatorname{Gal}(K/\mathbf{Q})| = 8$. At the finite level, balancing what we think we know about automorphisms with what we actually know is nicer due to the Galois correspondence of subfields of K to subgroups of $\operatorname{Gal}(K/k)$.

In the infinite-degree case, this Galois correspondence holds only for a special class of subgroups of $\operatorname{Gal}(K/k)$; it turns out that $\operatorname{Gal}(K/k)$ has a natural (albeit weird) compact Hausdorff topology, and going back and forth in the correspondence is akin to taking the closure. But in the finite case, this topology is discrete.

---

[21] There are actually theorems in complex differential geometry (related to Shigefumi Mori's Fields medal work) that are proven in characteristic p, with algebraic geometry.

[22] This is proven in the handout at `http://math.stanford.edu/~conrad/210BPage/handouts/insepdegree.pdf`; see Example 3.2.

The relationship between the fundamental group $\pi_1(X, x_0)$ and the absolute Galois group $\mathrm{Gal}(k_s/k)$ is explained more in a handout.[23] For example, there are commonalities in their cohomologies. One shadow of this is that as a sort of example, for the fundamental group, varying the basepoint leads to a sort of conjugation ambiguity, i.e. $\pi_1(X, x_0) \cong \pi_1(X, x_1)$, but the choice of isomorphism depends on conjugation, a path σ from x_0 to x_1, especially if not all such paths are homeomorphic; then, the isomorphism is in no sense canonical. Moreover, this becomes invisible on the abelianization $\mathrm{H}_1(X, \mathbf{Z})$ and its $\mathbf{Z}$-dual $\mathrm{H}^1(X, \mathbf{Z})$, i.e. the homology and cohomology.

The analogue for absolute Galois groups (i.e. $\mathrm{Gal}(k_s/k)$) is that given two separable closures k_s and k_s' and $\sigma, \tau : k_s \xrightarrow{\sim} k_s'$, $\mathrm{Gal}(k_s/k) \cong \mathrm{Gal}(k_s'/k)$ via either σ or τ, and these isomorphisms are related by conjugation by $\tau^{-1}\sigma$. This connection is no coincidence, ultimately related to something called the étale cohomology of a field.

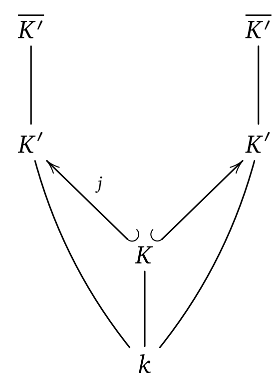
The point is that the absolute Galois group is as important as the fundamental group is in topology. Writing it down is hard, so people might study representations of it, which are insensitive to conjugation ambiguity.

Today, we're going to talk about infinite Galois theory. Often, people build up the infinite case from the finite one with inverse limits and such, but we can just do it directly.

Consider a general Galois extension K'/k and K/k with $j : K \hookrightarrow K'$ over k such that K'/K is Galois; then, we have $\mathrm{Gal}(K'/K) \subset \mathrm{Gal}(K'/k)$ (since automorphisms of K' fixing K must also fix k). Given an automorphism of K'/l, it can be composed with j to obtain other embeddings: $\mathrm{Gal}(K'/k) \to \mathrm{Hom}_k(K, K')$ given by $\gamma \mapsto \gamma \circ j$. This bijection yields $\psi : \mathrm{Gal}(K'/k)/\mathrm{Gal}(K'/K) \hookrightarrow \mathrm{Hom}_k(K, K')$.[24]

Claim. ψ is an equality, i.e. $\mathrm{Gal}(K'/k)$ acts transitively on the set of k-embeddings $K \hookrightarrow K'$.

Proof. In the following diagram, $\overline{K'}$ is realized as an algebraic closure of K in two ways:



Thus, it's realized by an isomorphism $\overline{\gamma} : \overline{K'} \to \overline{K'}$. $\overline{\gamma}$ fixes K, but since $K \hookrightarrow K'$ over k, then it also fixes k. But since K'/k is Galois, then $\overline{\gamma}$ must restrict to a k-isomorphism $\gamma : K' \xrightarrow{\sim} K'$ (i.e. $\overline{\gamma}$ sends K' to itself, though not necessarily as the identity). Thus, it carries j' to j, or maybe vice versa. ⊠

Corollary 9.1. *By the counting criterion for separability,* $[K' : k]$ *is finite iff* $\#\,\mathrm{Hom}(K, K')$ *is finite iff* $\mathrm{Gal}(K'/K)$ *has finite index in* $\mathrm{Gal}(K'/k)$*, in which case the group index is* $[K : k]$.

As a matter of notation, with K'/k understood, define $\Gamma_K = \mathrm{Gal}(K'/K) \subset \mathrm{Gal}(K'/k)$ (the intermediate group). Then, clearly, $K \subset (K')^{\Gamma_K}$. Going from the field to the group to the field is pretty easy; the other direction, though, is not as simple.

Claim. $K = (K')^{\Gamma_K}$, and in particular, for $k \subseteq K_1, K_2 \subseteq K$, $K_1 \subseteq K_2$ iff $\Gamma_{K_1} \supseteq \Gamma_{K_2}$.

Proof. We just have to check that for an $a \in K' \setminus K$, there exists an automorphism $\gamma \in \Gamma_K$ such that $\gamma(a) \neq a$. Notice this has nothing to do with k: just K'/K, so we can make the argument with the infinite case without arguments about compactness or the Krull topology.

The entire content of the proof is that $\mathrm{Gal}(K/K) \supsetneq \mathrm{Gal}(K'/k)$, but we just saw this; now, treating K as the ground field, it has index $[K' : K] > 1$. ⊠

A key example: suppose that $k \subseteq K \subseteq K'$. Then, by the normality criterion (all the ways of putting K/k into K', given one, since K/k is normal), then K/k is Galois if all $j \in \mathrm{Hom}_k(K, K')$ have the same image. Since they're all given by one, this is equivalent to requiring that for all $g \in \mathrm{Gal}(K'/k)$, $g(K) = K$, which is also equivalent

[23] `http://math.stanford.edu/~conrad/210BPage/handouts/Galpi1.pdf`.

[24] Note that $\mathrm{Gal}(K'/k)/\mathrm{Gal}(K'/K)$ denotes merely the coset space; $\mathrm{Gal}(K'/K)$ is not normal in general!

to requiring that for all $g \in \mathrm{Gal}(K'/k)$, $\Gamma_{g(K)} = \Gamma_K$. Since $\Gamma_{g(K)} = g\Gamma_K g^{-1}$, then it's only necessary to check the last equivalence, so an intermediate field K in a Galois extension K'/k is itself Galois over k iff $\Gamma_k \lhd \mathrm{Gal}(K'/k)$ (i.e. it's a normal subgroup), and when this happens, $\mathrm{Hom}_k(K, K') = \mathrm{Hom}_k(K, K) = \mathrm{Aut}_k(K)$, and furthermore, $\mathrm{Gal}(K'/k)/\mathrm{Gal}(K'/K) \cong \mathrm{Gal}(K/k)$ as groups, just because of how the map is defined.

This part goes exactly as in the finite case, which is nice. But the other direction is harder, yet often more useful. Suppose $H \subset \mathrm{Gal}(K'/k)$ is a subgroup. Then, if $K = (K')^H$, then $\mathrm{Gal}(K'/K) \supset H$, since H fixes the things fixed by it, but is it an equality? *Here, the general answer is 'no'*; there could be more things that preserve the thing fixed by H. Thus, we want to have a topology on $\mathrm{Gal}(K'/k)$ such that $\mathrm{Gal}(K'/K) = \overline{H}$, and the Galois correspondence holds in both directions for closed subgroups.

Example 9.1. Let k be finite of size q, so we have the q-Frobenius or arithmetic Frobenius $\varphi_q(x) = x^q$, which is an automorphism of $\overline{k}$ over k. There's also the geometric Frobenius $\varphi_q^{-1} : x \mapsto x^{1/q}$, which is uniquely defined in this characteristic.[25]

If $H = \langle \varphi_q \rangle \subset \mathrm{Gal}(\overline{k}/k)$, then $\overline{k}^H = k$ (which one can check at every finite level), but there are more automorphisms of $\overline{k}$ than $\varphi_{q^n} : x \mapsto x^{q^n}$ when $n \in \mathbf{Z}$.

Consider the set of finite subextensions ordered by divisibility: $\{k_n\}_{n|m}$. Then, to give an automorphism in $\mathrm{Gal}(\overline{k}/k)$, it's necessary to specify compatible automorphisms in $\mathbf{Z}/n\mathbf{Z}$ (since they indeed are Frobenius) with respect to reduction $\mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/d\mathbf{Z}$. Can one do this so that they don't stack nicely? The Chinese Remainder Theorem is compatible with reduction, so pick a prime ℓ and consider an $x_0 \in \mathbf{Z}_\ell \setminus \mathbf{Z}$ (i.e. an ℓ-adic integer, but not an ordinary one). Thus, take reductions of x_0 mod ℓ^e in the ℓ-part, and 0 in the other parts, and this becomes an automorphism, because an ℓ-adic number is just a set of compatible reductions; there's a huge number of potential choices, but writing down an explicit formula is hard.[26]

When we eventually define a topology in $\mathrm{Gal}(\overline{k}/k)$, $\mathbf{Z}$ will be dense in it, so taking the closure will work.

Now, in the finite-degree case, equality always holds, and in fact something nicer.

Lemma 9.2 (E. Artin). *Let L be any field, and $H \subset \mathrm{Aut}(L)$ be a finite subgroup. Then, L is finite Galois over L^H, with $H \xrightarrow{\sim} \mathrm{Aut}(L/L^H)$.*

The proof, which can be found in many books (e.g. Lang), is a beautiful application of the Primitive Element Theorem.

It's easy to see that L/L^H has to be algebraic, because

$$\prod_{h \in H} (X - h(a)) \in L^H[X]$$

for $a \in L$, but then $h \in H/\mathrm{Stab}_H(a)$, so it's even separable, and so forth. This is actually used to study stacks in algebraic geometry; the lemma makes the theory work in the finite case.

Tune in next time for the Krull topology.

10. The Krull Topology: 1/27/14

Look in §6.2 of Lang for applications of finite Galois theory (not constructing polynomials, though). Rather,

(1) Artin's 99% algebraic proof that $\mathbf{C}$ is algebraically closed, which does end up relying on the Intermediate Value Theorem in $\mathbf{R}$.

(2) The Symmetric Function Theorem: if $k(X_1, \ldots, X_n)^{S_n}$ denotes the elements of $k(X_1, \ldots, X_n)$ under the symmetric group, then $k(X_1, \ldots, X_n)^{S_n} = k(s_1, \ldots, s_n)$, with $s_1 = \sum x_i$, $s_2 = \sum x_i x_j$, and so on, with $s_n = \prod x_i$. In particular, these elementary symmetric functions $s_1, \ldots, s_n$ are algebraically independent over k.

(2') This theorem also has a ring-theoretic variant: if A be a commutative nonzero ring, then $A[X_1, \ldots, X_n] = A[s_1, \ldots, s_n]$, with the s_j algebraically independent over A.

After using facts in the theory of integrality to deduce (2') for $\mathbf{Z}$ from (2) for $\mathbf{Q}$, one can get (2') for general A with flatness considerations. Lang gives a direct proof, but it's uglier.

[25] The name here is due to the Lefschetz fixed-point formula for algebraic geometry objects; this is a cohomological formula for points over finite fields, and is more natural than it looks. Here, φ_q^{-1} pops up, whie φ_q is more common in number theory.

[26] An alternate way to do this is to add up factorials of numbers.

Norm and Trace. The norm and trace can and will be used in more general ring extensions, but first will be given in the field-theoretic case. Let K/k be finite, $a \in K$, and $m_a : K \to k$ be multiplication by a: $x \mapsto ax$. Then, define $\mathrm{Tr}_{K/k}(a) = \mathrm{trace}(m_a) \in k$ and $\mathrm{N}_{K/k}(a) = \det(m_a) \in k$. It will be shown that $\mathrm{Tr}_{K/k} : K \to k$ is k-linear, and that $\mathrm{N}_{K/k} : K \to k$ is multiplicative, i.e. $\mathrm{N}_{K/k}(ab) = \mathrm{N}_{K/k}(a)\mathrm{N}_{K/k}(b)$ and $\mathrm{N}_{K/k}(1) = 1$.[27] Note that, however, $\mathrm{Tr}_{K/k}(1) = [K : k] \in k$, so it may be zero in positive characteristic. More generally, if $c \in k$, then $\mathrm{Tr}_{K/k}(c) = c[K;k] \in k$ and $\mathrm{N}_{K/k}(c) = c^{[K:k]}$.

Example 10.1. Think about the case $K = k(a) = k[T]/(f)$, where $f(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_0 \in k[X]$. Using the ordered basis $\{1, a, \dots, a^{n-1}\}$, so that

$$a_n = -\sum_{n-1}^{n-1} c_i a^i,$$

then the matrix for m_a is

$$[m_a] = \begin{pmatrix} 0 & & & & -c_0 \\ 1 & 0 & & & -c_1 \\ 0 & 1 & 0 & & -c_2 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & -c_{n-1} \end{pmatrix},$$

and thus $\mathrm{Tr}_{k(a)/k}(a) = -c_{n-1}$ and $\mathrm{N}_{k(a)/k}(a) = (-1)^n c_0$. Informally, if $k(a)/k$ is separable, then the norm is the product of the conjugates (roots), and the trace is the sum.

Note that if $k(a)/k$ is purely inseparable, then $f = g(X^p)$, so $c_{n-1} = 0$, and thus $\mathrm{Tr}_{k(a)/k} = 0$. Transitivity will allow this to be broadened to general inseparable extensions.

Theorem 10.1.

(1) $\mathrm{Tr}_{K/k} \neq 0$ *iff K/k is separable.*[28]

(2) If K'/K and K/k, then $\mathrm{Tr}_{K'/k} = \mathrm{Tr}_{K'/K}\mathrm{Tr}_{K/k}$ *and* $\mathrm{N}_{K'/k} = \mathrm{N}_{K'/K} \circ \mathrm{N}_{K/k}$.

For example, we can use this to expand and put a in the ground field:

$$\mathrm{Tr}_{K/k}(a) = \mathrm{Tr}_{k(a)/k}(\mathrm{Tr}_{K/k(a)}(a)) = -[K : k(a)] \cdot c_{n-1},$$

where c_{n-1} is the $(n-1)^{\text{th}}$ coefficient in the minimal polynomial for a over k.

These results are useful for calculations, but it's a good thing they're not the definition, or else nobody would be able to prove anything.

Theorem 10.1 is proved in a handout;[29] the key to the proof is to do some normal closure and separability stuff to reduce to the Galois case, and then provide a nice formula which is useful for intuition. Specifically, if K/k is Galois and $G = \mathrm{Gal}(K/k)$, then

$$\mathrm{Tr}_{K/k}(a) = \sum_{g \in G} g(a) \qquad \text{and} \qquad \mathrm{N}_{K/k}(a) = \prod_{g \in G} g(a).$$

That is, it sums the roots with multiplicity (which comes into play when $k \subseteq k(a) \subsetneq K$).

The Galois-theoretic approach makes demonstrating transitivity really easy, but it has no use in the case of ring extensions.

Exercise 10.1. Prove the transitivity of the trace (reasonable) or the norm (hard) in the case of module-finite ring extensions.

These aren't linear-algebraic statements, so they can't be reduced to fields.

Here are two consequences of Theorem 10.1:

(1) If K/k is separable, there is a canonical k-bilinear form $K \times K \to k$ sending $(x, y) \mapsto \mathrm{Tr}_{K/k}(xy)$, and this form is symmetric and nondegenerate. This is called the trace pairing, especially for $k = \mathbf{Q}$ and K is a number field; its signature encodes information about K and thus is a particularly useful invariant.

(2) If K/k is Galois, then for $H \subset \mathrm{Gal}(K/k)$, $\mathrm{Tr}_{K/K^H} : K \twoheadrightarrow K^H$; it's surjective because it's linear and nonzero, and so forth... thus, $x \mapsto \sum_{h \in H} h(x)$ produces all of K^H. Thus, if one wants to understand K^H, a good place to start is picking $x \in K$ and seeing what happens.[30]

[27] These definitions do make sense for a commutative ring k and free k-algebra K, but the proofs of these facts then become much less obvious.

[28] This is only interesting if $\mathrm{char}(k) \mid [K : k]$, but in this case is very useful for constructing nondegenerate bilinear forms on a field extension.

[29] `http://math.stanford.edu/~conrad/210BPage/handouts/normtrace.pdf`.

[30] This works just as well for the product, but it's less easy to compute.

The Krull Topology. Now, we can discuss the Galois correspondence in the case where $[K:k]$ might be infinite. Let K'/K and K/k, $\Gamma = \mathrm{Gal}(K/k)$, and $\Gamma_K = \mathrm{Gal}(K'/K)$. Pick a subgroup $H \subset \Gamma$ such that $K = (K')^H$. We saw that $H' = \Gamma_K \supseteq H$, but this might be a strict inclusion (i.e. $H \neq \Gamma$, but $(K')^H = k$ sometimes). How can we tell when $H' = H$ or $(H')' = H'$?

There will be a natural topology on Γ here making it into a compact topological group, under which H' is the closure of H. In the finite case, this becomes the discrete topology, and in general, the Galois correspondence is just the quotient topology!

The collection of finite Galois subextensions of K'/k is directed under inclusion, because any two lie in a third, their compositum, and these exhaust K! In particular,

$$K = \bigcup_{\substack{L/k \\ \text{directed}}} K \cap L = \bigcup_{L/k} L^H,$$

where $K = (K')^H$. (The directed union is in fact the directed limit, but also the regular union.) Then, $H' = \Gamma_K = \{\gamma \in \Gamma \mid \gamma \text{ fices each } K \cap L = L^H\}$. Let H_L be the image of H in $\mathrm{Gal}(L/k)$; then, by finite Galois theory, $H' = \{\gamma \in \Gamma \mid \gamma|_L \text{ fixes pointwise } L^{H_L}\}$, or equivalently, $\gamma|_L \in H_L$, by *finite* Galois theory. This is the main content: a more useful way to think about it is that an automorphism of an infinite Galois extension is a set of compatible automorphisms of finite Galois extensions. Some presentations just throw the inverse limit topology, which isn't very easy to understand. The upshot is, $H' = \{\gamma \in \Gamma \mid \gamma|_L \in \mathrm{restr}_L(H)\}$ (where restr denotes restriction). γ looks like it lies in all H at each finite layer, though which element it comes from may change. Thus, it's not clear if γ itself comes from H, because which element it comes from can change.

As an analogue, consider how $e^x = \sum x^j/j! \in \mathbf{Q}[\![X]\!]$ is *not* in $\mathbf{Q}[X]$, but modulo each X^n is comes from $\mathbf{Q}[X]$.

Observation.

$$\mathrm{Gal}(K'/k) = \left\{ (g_L) \in \prod_{L/k} \mathrm{Gal}(L/k) \mid L_1 \subset L_2, g_{L_2}|_{L_1} = g_{L_1} \right\}.$$

To give an automorphism of the whole Galois extension, you just need to specify finite automorphisms at every finite layer, compatible under restriction. This is possible because the finite extensions are directed.

Now, just give this the subspace topology from the product topology, where each finite extension has the discrete topology. These conditions in the product space are closed conditions, and therefore $\mathrm{Gal}(K'/k)$ is a closed subspace, and therefore a compact Hausdorff topological group. Because of the directed condition, a lot of coordinate-messiness can be avoided with one later coordinate, in the sense that a base of open neighborhoods of a $\gamma \in \mathrm{Gal}(K/k)$ is exactly the things which agree with it on some L: $\gamma \cdot \Gamma_L = \{g \in \Gamma \mid g|_L = \gamma|_L \text{ on some } L\}$.

This topology is called the Krull topology, and can also be seen as $\mathrm{Gal}(K/k) = \varprojlim_L \mathrm{Gal}(L/k)$ with the inverse limit topology. But who cares?

On the homework, we'll polish off the remaining bits of this theory: that H' is the closure of H under this topology, and that there is a Galois correspondence for closed subgroups.

This topology isn't at all like a manifold; it's built up from finite layers, more like the p-adic numbers (since $\mathbf{Z}_p = \varprojlim_n \mathbf{Z}/p^n$); for example, it's totally disconnected.

Here are some more nice results about the Krull topology.

(1) For intermediate K Galois over k, $\mathrm{Gal}(K'/k)/\mathrm{Gal}(K'/K) \to \mathrm{Gal}(K/k)$ is a continuous (and we already knew it was a bijection), and both sides are compact Hausdorff. From topology one has the following lemma:

Lemma 10.2. *A continuous bijection between compact Hausdorff topological spaces is a homeomorphism.*

Thus, the topological operations on the Galois group are compatible with the algebraic ones.

(2) A closed subgroup $H \subset \Gamma$ of finite index is open, because

$$\Gamma = \coprod_{\text{finite}} \gamma_i \cdot H,$$

and therefore the complement is also closed. Likewise, since Γ is compact, all open subgroups have finite index; it's amusing, but useful, to invoke a finite cover by disjoint translates, which are open, so their union is open, and therefore the complement is closed.

That is, finite subextensions correspond to open (equivalently closed) subgroups of finite index. There's lots of fun to be had here; this is functorial, etc.

Part 2. **Affine Algebraic Geometry**

11. Affine Algebraic Sets and Radical Ideals: 1/29/14

Even purely field-theoretic statements in Galois theory have counterparts in differential geometry, which suggest interesting ways to approach them. This relates to an idea called Galois cohomology, which this course will approach towards the end of the quarter.

Suppose K/k is finite Galois and has Galois group G. Then, G acts on $\mathrm{GL}_n(K)$, componentwise, and the fixed points are $\mathrm{GL}_n(K)^G = \mathrm{GL}_n(k)$. But what does it do to the projective general linear group $\mathrm{PGL}_n(K) = \mathrm{GL}_n(K)/K^\times$?[31] Then, $\mathrm{GL}_n(k) \hookrightarrow \mathrm{GL}_n(K)$ induces $\mathrm{PGL}_n(k) \hookrightarrow \mathrm{PGL}_n(K)$. This induces $\mathrm{PGL}_n(k) \hookrightarrow \mathrm{PGL}_n(K)^G$, and in fact equality holds, though this requires something called Hilbert's Theorem 90 to show.

Similarly, look at the case of $\mathrm{SL}_n(k)$, as long as $k \neq \mathbf{F}_2$ or $\mathbf{F}_3$. Its center is $\mu_n(k)$, and so one defines $\mathrm{PSL}_n(k) = \mathrm{SL}_n(k)/\mu_n(k)$. Does $\mathrm{PSL}_n(k) \hookrightarrow \mathrm{PSL}_n(K)^G$? In general, no! There's a cohomological obstruction to this, which has to do with the Brauer group of associative algebras over k.

As a kind of analogue to this, $\mathrm{GL}_n(\mathbf{R})$ is a real manifold, so $\mathrm{GL}_n(\mathbf{R}) \to \mathrm{PGL}_n(\mathbf{R})$ is what's known as a line bundle or $\mathbf{R}^*$-torsor. This means that given a manifold M and a C^∞-map $M \to \mathrm{PGL}_n(\mathbf{R})$, it can be lifted to a map $M \to \mathrm{GL}_n(\mathbf{R})$ iff M has nontrivial line bundles. The reason $\mathrm{PGL}_n(k) \xrightarrow{\sim} \mathrm{PGL}_n(K)^G$ is because all k-vector spaces have bases, so $\mathrm{Spec}(k)$ has no nontrivial line bundles. But in the more general case of ring extensions, this doesn't hold.

Though this might be a bit bewildering, the point is that in affine algebraic geometry, one can talk about seemingly purely algebraic questions with geometric methods.

In commutative algebra, one wants to be able to visualize these concepts about rings and modules. Thus, a set of analogies exists; for these analogies, don't worry about the critical details, but instead the intuition.

- There should be some nice correspondence of rings $\longleftrightarrow$ manifolds, where the ring is the ring of total functions of the manifold.
- Ideals $\longleftrightarrow$ submanifolds, corresponding to zero sets of equations or functions.
- Modules $\longleftrightarrow$ vector bundles over the manifold, via something called "sheaves."

The point is, there should be a way of geometrizing algebraic objects. For example, if A is a commutative ring and M is a finitely generated A-module, then for all primes $\mathfrak{p}$ of A, one obtains a vector space $M(\mathfrak{p}) = M \otimes_A \mathscr{K}(\mathfrak{p})$ over $\mathscr{K}(\mathfrak{p}) = \mathrm{Frac}(A/\mathfrak{p}) = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$.[32] So there's this family of vector spaces, akin to a vector bundle.

The ur-example is that we want the algebraic object $k[X_1, \dots, X_n]$ to correspond to the geometric object k^n, affine n-space over k. There are some issues with the correspondence if k is finite or not algebraically closed. If $f \in k[X_1, \dots, X_n]$, then one has a function $[f] : k^n \to k$ sending $\underline{X} \mapsto f(\underline{X})$. Notice that this ignores the linear structure of k^n (hence affine space).

Here are some issues with this correspondence.

(0) If k is finite, then $[f]$ doesn't determine f.

(1) If $k \neq \overline{k}$, then a nonconstant $f \in k[X_1, \dots, X_n]$ might have an empty zero locus in k^n.

Because of the latter concern, we will consider zeros with coordinates in $\overline{k}^n$. This in some sense is a loss of information, but it's not a huge deficit.

The notation $k[\underline{X}]$ is understood to mean $k[X_1, \dots, X_n]$ for some n which is fixed within the context of the discussion.

Definition. Given an ideal $J \subset k[\underline{X}]$, the zero locus of J is $\underline{Z}(J) = \{\underline{X} \in \overline{k}^n \mid h(\underline{X}) = 0 \text{ for all } h \in J\}$.

By the Hilbert Basis theorem, every ideal of $k[\underline{X}]$ is finitely generated, so the zero locus of J is the common zero locus of its generators $h_1, \dots, h_r$.

Another way of thinking about these zeros is in terms of maps: $\underline{Z}(J) = \mathrm{Hom}_{k\text{-alg}}(k[\underline{X}]/K, \overline{k})$ via $z \mapsto (f \mapsto f(z))$, which is well-defined exactly when $z \in \underline{Z}(J)$, so that $f \mapsto 0$ if $f \in J$. Correspondingly, if $k[\underline{X}]/J \to \overline{k}$ sends $X_i \mapsto c_i \in \overline{k}$, or equivalently $f \mapsto f(\underline{c})$, then one obtains the corresponding point $(c_1, \dots, c_n) \in \overline{k}^n$.

As with Galois theory, is there a correspondence? Starting with a subset of $\overline{k}^n$, does one obtain ain ideal? This will be addressed later. Right now, though, we can ask whether it's possible to reconstruct $J \subset k[\underline{X}]$ from $\underline{Z}(J) \subset \overline{k}^n$, i.e. if $\underline{Z}(J) = \underline{Z}(J')$, does $J = J'$?

Clearly, from the definition, if $J \subseteq J'$, then $\underline{Z}(J') \subseteq \underline{Z}(J)$. The converse, however, is false. A (silly-looking but serious) obstruction is that $\underline{Z}(J^2) = \underline{Z}(J)$. The most basic example is that if J is principal, so that $J = (f)$, where

[31] This definiton is functorial over K, but isn't the best. Equivlently, one could describe it as modding out by the center of $\mathrm{GL}_n(K)$, or as $\mathrm{Aut}_k(\mathbf{P}_k^{n-1})$, whatever that is.

[32] This is a pretty typical construction in commutative algebra, used to answer quesitons about the module M.

$f = c\prod_i^{e_i}$, where the h_i are pairwise non-associate irreudicibles, is that $\underline{Z}(J) = \underline{Z}(\prod h_i)$. This means that the zero locus throws out quite a lot of information about multiplicities, so it's helpful to pass to a class of ideals where this sort of thing is ivisible.

Definition. Let A be a commutative ring and $J \subseteq A$ be an ideal. Then, the radical of J is $\mathrm{rad}(J) = \{a \in A \mid a^e \in J \text{ for some } e > 0\}$.

J is radical if $J = \mathrm{rad}(J)$.

This is an ideal, using $(a'_a)^{e+e'}$ and the binomial theorem (since then each term is in $\mathrm{rad}(J)$). Then, we have that $J \subseteq \mathrm{rad}(J)$ even for non-radical J, and $\mathrm{rad}(0)$ is the set of nilpotent elements.

In the case $A = k[\underline{X}]$, if f factors as $f = c \cdot \prod h_i^{e_i}$, then by the UFD property, $\mathrm{rad}(f) = (\prod h_i)$. Since $(a^e)^{e'} = a^{ee'}$, then $\mathrm{rad}(\mathrm{rad}(J)) = \mathrm{rad}(J)$, which means thar $\mathrm{rad}(J)$ is radical, which is fortunate.

Back in $k[\underline{X}]$-land, this illustrates that $\underline{Z}(\mathrm{rad}(J)) = \underline{Z}(J)$. Now, given radical ideals $J, J' \subseteq k[\underline{X}]$, does this containment work among the zero loci?

As a special case, if $\underline{Z}(J) = \emptyset$, then $\underline{Z}(J) \subseteq \underline{Z}(1)$, since $\underline{Z}(1) = \emptyset$, and this will end up being equivalent to the general case. In other words, if J is a proper ideal, is it necessarily the case that $\underline{Z}(J) \neq \emptyset$?

In a more (contra)positive way of thinking about this, using a finite generating set of J, suppose one is given $h_1, \dots, h_r \in k[\underline{X}]$. if $\underline{Z}(h_1, \dots, h_r) = \emptyset$, then do there exist $g_1, \dots, g_r \in k[\underline{X}]$ such that $\sum g_i h_i = 1$? The converse is true, because $0 \neq 1$.

Suppose $J \subset k[\underline{X}]$ is a proper ideal. Thus, it is contained in a maximal ideal $\mathfrak{m}$.[33] Thus, $k[\underline{X}]/J \twoheadrightarrow k[\underline{X}]/\mathfrak{m}$ as k-algebras. $k[\underline{X}]/\mathfrak{m}$ is a field, so can we stuff it into $\overline{k}$? Unlike $k[T]$, $k[\underline{X}]/\mathfrak{m}$ is finitely generated as an *k-algebra*, even though both are finitely generated field extensions. The distiction is akin to how $\mathbf{Q}$ isn't a finitely generated $\mathbf{Z}$-algebra. If $k[\underline{X}]/\mathfrak{m}$ is a finite extension, then it can be embedded in $\overline{k}$, so the question reduces to whether it's finite (as fields) over k.

In the nicest, too-good-to-be-true case, $k[\underline{X}]/\mathfrak{m} \xleftarrow{\sim} k$. Then $(c_1, \dots, c_n) \in \underline{Z}(J)$ iff $c_i \mapsto X_i$, i.e. $X_i - c_i \in \mathfrak{m}$. Then, $\mathfrak{m} = (X_1 - c_1, \dots, X_n - c_n)$, and everything in J is a polynomial in these $X_i - c_i$.

Theorem 11.1 (Weak Nullstellensatz[34]). *If K/k is a field extension that is finitely generated as a k-algebra, then it is a finite field extension. Thus, if k is algebraically closed, then $K = k$.*

It's pretty clear in the $k[\underline{X}]/\mathfrak{m}$ case that this holds, but the presence of transcendental elements can make this weird. In any case, a proof will be given next lecture.

Corollary 11.2. *If k is algebraically closed, then the maximal ideals of $k[X_1, \dots, X_n]$ are $(X_1 - c_1, \dots, X_n - c_i)$ for $(c_1, \dots, c_n) \in k^n$.*

This is shown by looking at the map $k \xrightarrow{\sim} k[X_1, \dots, X_n]/\mathfrak{m}$, sending $c_i \mapsto X_i$.

This has one very interesting consequence.

Corollary 11.3. *If $h_1, \dots, h_r \in k[X_1, \dots, X_n]$ have a common zero in some algebraically closed extension K/k, then they have a common zero in a finite extension (equivalently, in $\overline{k}^n$).*

Proof. Let $J = (h_1, \dots, h_r) \subset k[\underline{X}]$, so $K \otimes_k J \subset K[\underline{X}]$ is also generated by the h_i. Thus, by tensor magic over fields, $J = (1)$ iff $K \otimes_k J = (1)$. ⊠

For example, for polynomials in $\mathbf{Q}[\underline{X}]$, any polynomials with a common zero over $\mathbf{C}$ in common will have it over $\overline{\mathbf{Q}}$.

12. The Nullstellensatz: 1/31/14

Recall the weak Nullstellensatz: that if k is a field and K is an extension field finitely generated as a k-algebra (equivalently, $K = k[X_1, \dots, X_n]/\mathfrak{m}$ for a maximal ideal $\mathfrak{m}$), then $[K : k]$ is finite.

The simplest non-example is the simplest transcendental extension $K = k(T)$. An actual example is, if k is an algebraically closed field, then $k \xrightarrow{\sim} k[\underline{X}]/\mathfrak{m}$, where $\mathfrak{m} = (X_1 - c_1, \dots, X_n - c_n) = \{f \in k[X] \mid f(\underline{c})0\}$ and $c_i \mapsto X_i$. Here, $\mathfrak{m}$ is the prime ideal of functions that vanish at $\underline{c}$: prime ideals correspond to points.

Proof of Theorem 11.1. In this proof, we can't rely on k to be algebraically closed, because that would be too weak for the induction. The induction will be on n, where $K = k[a_1, \dots, a_n] = k[X_1, \dots, X_n]/\mathfrak{m}$. Notice that $\mathfrak{m} \neq (0)$, because $k[X_1, \dots, X_n]$ isn't a field.

[33]There's no need to mess with Zorn's lemma or colimits in this case, because $k[\underline{X}]$ is Noetherian.

[34]The pronunciation is [nʊlʃteːleːnzats]. The word literally means "zero places theorem."

If $n = 1$, then $\mathfrak{m} = (f)$ for some monic irreducible f, so $[K : k] = \deg(f)$ is finite.

Suppose $n > 1$; then, we want all of the a_i to be algebraic over k. Suppose not, so without loss of generality a_1 is transcendental over k. Then, because K is a field, then $K = k[a_1, \dots, a_n] = k(a_1)[a_2, \dots, a_n]$. Thus, this field is finitely generated as a $k(a_1)$-algebra. Apply induction with the ground field $k(a_1) \cong k(T)$ (which is why the induction isn't over an algebraically closed field), so $a_2, \dots, a_n$ are algebraic over $k(T)$, and thus K is module-finite (i.e. finitely generated as a module) over $k(T)$. Thus, each $a_2, \dots, a_n$ has a minimal polynomial, respectively $p_2, \dots, p_n \in k(T)[Y]$ (and probably not in $k[T, Y]$).

The idea to use here is that any finite number of things in $k(T)$ share a common denominator, but that there's alqays something that doesn't match it. Let $\Delta \in k[T]$ be a common denominator of the $k(T)$-coefficients of the p_j; theus, there is a big exponent e such that $\Delta^e a_2, \dots, \Delta^e a_n$ satisfy monics over $k[T]$, e.g.

$$p_2(T, W) = y^d + \frac{c_{d-1}(T)}{\Delta} y^{d-1} + \cdots + \frac{c_0(T)}{\Delta}$$

for some $c_i \in k[T]$. Thus, $\Delta^d p_2 = q_2(\Delta \cdot Y)$, where q_2 is monic over $k[T]$, and $q_2(\Delta a_2) = 0$. These are a bit nicer to deal with: let $a_2' = \Delta a_2$, and so on; as far as $k(T)$-algebra generators, one can use $a_2', \dots, a_n'$ in place of $a_2, \dots, a_n$. Thus, $K = k(T)[a_1', \dots, a_n']$, and this means we only need to invert Δ, so $K = k[T, 1/\Delta][a_2', \dots, a_n']$. This is still module-finite over $k[T, 1/\Delta]$, so one can use the monic relations so that the exponents needed are only up to the degrees of the minimal polynomials.

Now, this is already sounding alarming, because K is a field. But over rings like this one, submodules of finitely generated modules are finitely generated, which is good. This, the intermediate $k[T, 1/\Delta]$-module $k(T)$ must also be module-finite — but we already know this to not be true for any $\Delta \neq 0$. The point is, $k(T)$ is a field, but $k[T, 1/\Delta]$ is not. This can be proven by hand, but it follows from the more general result:

Proposition 12.1. *Suppose A is a Noetherian domain that is not a field. Then,* $\mathrm{Frac}(A)$ *is not A-finite.*[35]

Proof. As we'll see later on in the class, the Noetherian assumption is actually unnecessary; it just makes the proof shorter in this case. The idea is to get a noninvertible element, take its reociprical, and look at powers of it.

Choose an $a \in A \setminus \{0\}$ and such that $1/a \notin A$. Then, consider $A[1/a] \subset \mathrm{Frac}(A)$ (i.e. the A-span of $1/a, 1/a^2, \dots$). Assume $\mathrm{Frac}(A)$ is A-finite. Then, since A is Noetherian, then $A[1/a]$ must also be A-finite, since submodules of finitely generated Noetherian modules must be finitely generated. (Think of the special case $\mathbf{Z}[1/7]$, which isn't finitely generated over $\mathbf{Z}$: you need a unit.)

Thus, $A[1/a]$ is spanned over A by $\{1, 1/a, \dots, 1/a^n\}$ for some n. Great: now, $1/a^{n+1} \in A[1/a]$, so it must be an A-linear combination

$$\frac{1}{a^{n+1}} = c_0 + \frac{c_1}{a} + \frac{c_2}{a^2} + \cdots + \frac{c_n}{a^n}$$

for some $c_i \in A$, and therefore

$$1 = c_0 a^{n+1} + c_1 a^n + \cdots + c_n a = a\underbrace{\left(c_0 a^n + c_1 a^{n-1} + \cdots + c_0\right)}_{\in A},$$

so a is a unit after all! ⊠

(This was kind of a gratuitous proof by contradiction; it's possible to reword it to be more direct.)

Thus, the Weak Nullstellensatz follows. ⊠

This theorem implies results such as that if six polynomials in $\mathbf{Q}[X]$ share a root in $\mathbf{C}$, then that root is in $\overline{\mathbf{Q}}$. However, the proof is indirect and ideal-theoretic: since the ideal is proper, then it must vanish at a point.

For the rest of this lecture, assume that k is algebraically closed.

Definition. An affine algebraic set in k^n is the zero locus of some ideal: $\underline{Z}(J)$, where $J \subseteq k[X_1, \dots, X_n]$ is an ideal. Given any subset $S \subset k^n$, one has $\underline{I}(S) = \{f \in k[X_1, \dots, X_n] \mid f(s) = 0 \text{ for all } s \in S\}$.

$\underline{I}(S)$ is not just an ideal of $k[X_1, \dots, X_n]$, but a radical ideal; since $\underline{Z}(J) = \underline{Z}(\mathrm{rad}\, J)$, then this association might as well be in terms of radical ideals.

Example 12.1.

- $\underline{I}((c_1, \dots, c_n)) = (X_1 - c_1, \dots, X_n - c_n)$.
- $\underline{I}(\emptyset) = (1)$. This might be true on its own, or maybe it's just a convention. In either case, it makes stuff work.
- $\underline{I}(k^n) = (0)$.
- $\underline{I}(\{X_1 = 0\}) = \{h \in k[\underline{X}] \mid h(0, X_2, \dots, X_n) = 0\} = (X_1)$.

[35]This means $\mathrm{Frac}(A)$ isn't finitely generated as an A-module.

More generally, if $f \in k[\underline{X}]$ is irreducible, then $\underline{I}(\{f=0\}) \supseteq (f)$. It turns out that equality will hold…

Theorem 12.2 (Nullstellensatz). $\underline{I}(\underline{Z}(J)) = \operatorname{rad}(J)$.

We already knew that $\underline{I}(\underline{Z}(J)) \supseteq \operatorname{rad}(J)$ and that it was radical, but the full theorem follows from an artful application of the weak Nullstellensatz. The implication is that $\underline{Z}$ and $\underline{I}$ are inverse, inclusion-reversing bijections between sets of radical ideals of $k[X_1,\dots,X_n]$ and affine algebraic sets.

It's meaningful to ask this over k not algebraically closed, going up to $\overline{k}$ and seeing what happens. But this messes with radicals: if k isn't perfect, then $J \subset k[X_1,\dots,X_n]$ can be radical while $\overline{k} \otimes_k J \subset \overline{k}[\underline{X}]$ is *not* radical. e.g. if $\operatorname{char}(k) = p > 0$, $a \in k \setminus k^p$ and $J = (X^p - a) \subset k[\underline{X}]$. Then, $\operatorname{rad}(\overline{k} \otimes_k J) = \overline{k} \otimes_k \operatorname{rad}(J)$.

Proof of Theorem 12.2. The idea of the proof is to turn the locus where an $f \in \underline{I}(\underline{Z}(J))$ is not zero into an affine algebraic set in k^{n+1} via an extra variable. In $k[X_1,\dots,X_n,T]$, consider $Tf-1$, and let $B = k[X_1,\dots,X_n,T]/(J, Tf-1)$.

By hypothesis, i.e. that $f|_{\underline{Z}(J)} = 0$, there's no common solution, so there is no k-algebra map $B \to k$. But that's weird, because B is a finitely generated k-algebra, so by the weak Nullstellensatz, for any maximal ideal $\mathfrak{m}$ of B, $B/\mathfrak{m} \xleftarrow{\sim} k$ as k-algebras.[36] Thus, B can have no maximal ideals! So $B = (0)$.

But if $A = k[\underline{X}]/J$, then $B = A_f$, i.e. the localization of A at f (or, technically, at $\overline{f}$, the class of f). Since f becomes 0 in the localization, then $\overline{f}$ must be nilpotent: $1 = 0$ in $A_{\overline{f}}$, so $\overline{f}^n(1-0) = 0$. But that just means some $f^n \in J$! ⊠

In summary, $f|_{\underline{Z}(J)} = 0$, so $\underline{Z}(J)$ is disjoint from $\{f \neq 0\}$. This trick, called the Rabinowitz trick, involves turning nonzero sets into zero sets. Hilbert's original proof of the Nullstellensatz was probably more geometric.

13. MaxSpec and Friends: 2/3/14

Recall that for general k, $\underline{I}(\underline{Z}(J)) = \operatorname{rad}(J)$ in $k[\underline{X}]$ (though $\underline{Z}(J) \in \overline{k}^n$) using $\operatorname{Hom}_{k\text{-alg}}(k[\underline{X}]/J, \overline{k})$, as in the proof of the weak Nullstellensatz. But once again assume that k is algebraically closed, so that the full Nullstellensatz holds and there is a bijection between k^n and the maximal ideals of $k[X_1,\dots,X_n]$ realized by sending $(c_1,\dots,c_n) \mapsto (X_1 - c_1,\dots,X_n - c_n)$, and in the opposite direction, $\mathfrak{m} \mapsto (k \xrightarrow{\sim} k[X_i]/\mathfrak{m})$, where the latter map sends $c_i \mapsto X_i \bmod \mathfrak{m}$.

Within functional analysis there's a beautiful thing called the Gelfand transform, under which the maximal ideals of the ring of continuous global functions of a compact Hausdorff space have a natural topology isomorphic to that of the original space. This idea is similar: that the maximla ideals have a natural geometric structure.

Definition. For any ring A, $\operatorname{Spec}(A)$ is the set of prime ideals of A and $\operatorname{MaxSpec}(A)$ is the set of maximal ideals of A.

The idea is that in the case where A is finitely generated over a field, $\operatorname{MaxSpec}(A)$ is a "geometric object," for which A is more or less its field of global functions, in some topological sense. Note that for more general A, the "right" geometric object is $\operatorname{Spec}(A)$, which will be explained later in the course.

The issue is functoriality: given $\varphi : A \to B$, one has $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ given by $\mathfrak{p} \mapsto \varphi^{-1}(\mathfrak{p})$. In the special cases we've been working with, the preimage of a maximal ideal is maximal, providing some additional geometric meaning; but this is in general not true. This is because subrings of fields might not be fields, just domains (e.g. $\mathbf{Z} \hookrightarrow \mathbf{Q}$), so $A/\varphi^{-1}(\mathfrak{m}) \hookrightarrow B/\mathfrak{m}$; for example, $\operatorname{Spec}(\mathbf{Q}) \to \operatorname{Spec}(\mathbf{Z})$, but $\operatorname{MaxSpec}(\mathbf{Q}) \not\to \operatorname{MaxSpec}(\mathbf{Z})$.

However, if A and B are finitely generated over a field F, then $B/\mathfrak{m}$ is F-finite (by the weak Nullstellensatz), and $A/\varphi^{-1}(\mathfrak{m}) \hookrightarrow B/\mathfrak{m}$ over F (i.e. as F-algebras). This means that $A/\varphi^{-1}(\mathfrak{m})$ is a field, and therefore $\varphi^{-1}(\mathfrak{m})$ is maximal.

All of the experience here is motivated by MaxSpec for finitely generated algebras over an algebraically closed field. This gives enough geometric intuition to carry over to the more general case.

Continuing, let k be an algebraically closed field. Then, the basic setup was the Nullstellensatz bijection $\{\text{radical ideals in } k[X_1,\dots,X_n]\} \leftrightarrows \{\text{affine algebraic sets in } k^n\}$ given by $J \mapsto \underline{Z}(J) = \operatorname{Hom}_{k\text{-alg}}(k[X_1,\dots,X_n]/J, k)$ (evaluation at a point, such that J is killed). This sits in k^n by way of the map $k[X_1,\dots,X_n] \twoheadrightarrow k[X_1,\dots,X_n]/J$, yielding the coordinates of the point. Here, it matters that A is presented as a quotient, not just a k-algebra. Then, the inverse is $\underline{I}(Z)$, and the Nullstellensatz guarantees there are inverse operators.

We want to use this dictionary to turn questions about ideals to questions about zero sets, which are easier to visualize. This is much like how on visualizes linear algebra.

Here are a few elementary properties of this bijection:

[36] This uses the fact that k is algebraically closed; perhaps you can deduce something more general.

(1)
$$\bigcap_\alpha \underline{Z}(J_\alpha) = \underline{Z}\left(\sum_\alpha J_\alpha\right),$$
where the sum on the right-hand side means finite sums of elements.

(2) $\underline{Z}(J) \cup \underline{Z}(J') = \underline{Z}(JJ')$, (i.e. the ideal generated by elements jj' for $j \in J$ and $j' \in J'$).

Already there's a nuisance: $\sum_\alpha J_\alpha$ and JJ' tend not to be radical. For example, in $k[X,Y]$, take $J_1 = (Y - X^2)$ and $J_2 = (Y)$. Their intersection is $\underline{Z}(J_1 + J_2) = \{(0,0)\}$, but $J_1 + J_2 = (Y, X^2)$ isn't radical (since $X \notin J_1 + J_2$).

This corresponds to Figure 1; the failure of the sum to be radical indicates that the curves intersect non-transversely.[37]

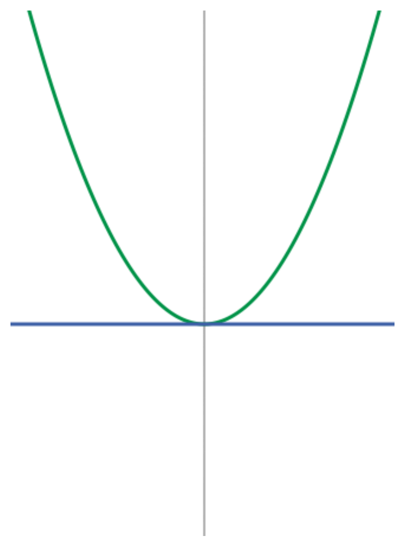


FIGURE 1. The affine algebraic sets $\underline{Z}(Y - X^2)$ and $\underline{Z}(Y)$ intersect non-transversely.

A counterexample to the second property (other than $J = J'$, which works, but is silly) is $J = (XY)$ and $J' = (X(X+Y))$. They have the Y-axis in common, but one has the X-axis while the other has the line $Y = X$. These three pieces can be thought of as irreudicble components, akin to the irreducible factors of a polynomial, but this will be defined more precisely later in the course.

One more property, useful even if it's fairly straightforward:

(3) $\underline{Z}(1) = \emptyset$ and $\underline{Z}(0) = k^n$.

These properties can be summarized by saying that the affine algebraic sets constitute the closed sets of a (weird, but useful) topology in k^n: the Zariski topology. This is in some sense a linguistic device: it's a weird topology, and *very* non-Hausdorff.

Applying the Nullstellensatz to these properties, one obtains two more:

(1')
$$\underline{I}\left(\bigcap_\alpha Z_\alpha\right) = \operatorname{rad}\left(\sum_\alpha Z_\alpha\right).$$

(2') $\underline{I}(Z \cup Z') = \operatorname{rad}(\underline{I}(Z) \cdot \underline{I}(Z'))$.

It would really be a pain to prove these directly, without the Nullstellensatz.[38]

On an affine algebraic set $Z \subset k^n$, the subspace topology induced from k^n is also the Zariski topology via radical ideals of $k[\underline{X}]/\underline{I}(Z)$: $Z' \subseteq Z$ iff (by the Nullstellensatz) $\underline{I}(Z') \supseteq \underline{I}(Z)$. One could define it intrinsically with the same procedure, but it's the same topology.

Example 13.1. Suppose $Z = \{(a,b),(a',b')\} \subset k^2$. Then,
$$\begin{aligned}\underline{I}(Z) &= \operatorname{rad}((X-a, Y-b)\cdot(X-a', Y-b'))\\ &= \operatorname{rad}((X-a)(X-a'), (X-a)(Y-b'), (X-a')(Y-b), (Y-b)(Y-b')).\end{aligned}$$

[37]This indicates that we really should be using schemes... but that's far beyond the scope of the course, and in particular, the qualifying exam.

[38]Once again, when one defines everything with schemes, this makes more sense, and the radicals go away. But that's another story.

In the case $a \neq a'$ and $b \neq b'$, then this is already radical. More interestingly, it's still true as long as the points are distinct in general, which is a degenerate case of transversality.

The open sets in the Zariski topology are *gigantic*, since they're complements of zero loci. In some sense, working in the Zariski topology is like trying to write with a pencil with a twelve-inch radius. Thus, having a basis for the topology will make it more tractable.

Lemma 13.1. *A base of the Zariski topology on k^n (or for any affine algebraic set $Z = \underline{Z}(J)$) is given by the basic opens $U_f = \{f \neq 0\}$ for $f \in k[\underline{X}]$ (resp. $f \in k[\underline{X}]/J$).*

Proof. Choose a point $z \notin Z(J)$, so that there is an $f \in J$ such that $f(z) \neq 0$. Then, $z \in U_f \subseteq k^n \setminus \underline{Z}(J)$. ⊠

After all, if $J = (f_1, \dots, f_n)$, then $\underline{Z}(J) = \bigcap\{f_i = 0\}$, so just take the unions of their complements. Additionally, this lemma has the consequence that this topology is *very* non-Hausdorff: $U_f \cap U_g = U_{fg} \neq \emptyset$ whenever $f, g \neq 0$.

For affine algebraic sets, there are irreducible components. We want to write each such affine algebraic set as a finite union of irreducible components, even if it was given by a non-principal ideal.

Example 13.2. If $J = (f)$ and $f \notin k$, then write $f = c \cdot \prod f_i^{e_i}$ with $c \in k^\times$ and the f_i pairwise distinct irreducibles. Then, $\underline{Z}(J) = \bigcup \underline{Z}(f_i)$, and there are no containment relations amongst the $\underline{Z}(f_i)$.

In the above example, the component sets have a property called irreducibility, which we'll define in a moment using the Zariski topology, and relate to algebra using (of course) the Nullstellensatz.

Definition. A topological space X is called Noetherian if it satisfies the descending chain condition for closed sets.

For example, affine algebraic sets are Noetherian, because $k[\underline{X}]$ satisfies the ascending chain condition for radical ideals (in fact, all ideals in $k[\underline{X}]/\underline{I}(Z)$ do). Note that a topological space is Noetherian if all of its subspaces are compact under the subspace topology, so any interesting manifold (i.e. not just a finite collection of points) isn't Noetherian.

Definition. A topological space X is irreducible if:

(1) $X \neq \emptyset$, and
(2) if $X = Z \cup Z'$ for closed sets $Z, Z' \subset X$. then $X = Z$ or $X = Z'$.

Given (1), (2) is equivalent to having that all nonempty open sets are dense. Of course, this is madness in any reasonable Hausdorff space that you might bring home to your mother.

Next time, we will use the magic of Noetherian induction to show that every Noetherian space decomposes into a finite union of irreducible spaces, in a vast generalization of factorization of polynomials.

However, we can already make interesting connections between this geometric notion of irreducibility and algebraic ideas.

Proposition 13.2. *For radical $J \subseteq k[\underline{X}]$, $\underline{Z}(J)$ is irreducible iff J is a prime ideal.*

Proof. In the forward direction, choose $a, b \in k[\underline{X}]$ such that $ab \in J$, and therefore ab vanishes on Z. Then, look at $\underline{Z}(J, a) \cup \underline{Z}(J, b) = \underline{Z}(J, ab) = \underline{Z}(J)$ (since the J^2 term vanishes after taking radicals). Since $\underline{Z}(J)$ is irreducible, but $J \neq (1)$ (since $\underline{Z}(J) \neq \emptyset$), then one of $\underline{Z}(J, a)$ and $\underline{Z}(J, b)$ must be equal to $\underline{Z}(J)$; without loss of generality, suppose it's $\underline{Z}(J, a)$. Then, $\mathrm{rad}(J, a) = \mathrm{rad}(J) = J$, because J is radical. ⊠

14. Noetherian Induction: 2/5/14

Recall that a Noetherian topological space is one which satisfies the descending chain condition on closed sets. These are just sequences, not posets: $Z_1 \supseteq Z_2 \supseteq Z_3 \supseteq \dots$ Eventually, we will define dimension for topological spaces which is reasonable for the Zariski topology. Some Noetherian topological spaces have infinite dimension, which is all right.[39]

The next theorem is a geometric analogue to unique factorization of polynomials.

Theorem 14.1. *Let X be a nonempty Noetherian topological space. Then, there exists a unique finite set $\{Z_i\}$ of irreducible closed subsets of X such that*

(1) $X = \bigcup_{i=1}^n Z_i$, and
(2) $\{Z_i\}$ is irredundant, i.e. $Z_i \not\subset \bigcup_{j \neq i} Z_j$ for all i.

[39] There's a fantastic book by Engelking that tells the beautiful story of dimension for nice topological spaces.

These Z_i are called the irreducible components of X, and are akin to the prime power factors of a polynomials. By the irredundancy condition, $Z_i - \bigcup_{j\neq i}(Z_j \setminus Z_i)$ is the Z_i-complement of a proper closed subset of the irreducible Z_i, so the entire set must be dense open in Z_i and disjoint from the other Z_i. It's huge!

The proof of Theorem 14.1 will be in a geometric style, even though it's basically a translation of the proof of unique factorization in $\mathbf{Z}$.

Remark. In the study of affine algebraic sets, which satisfy both the descending and ascending chain conditions on closed sets, the irreducible case is the most important. But the more general case is useful, and more robust with respect to intersections: two irreducible sets may intersect in a reducible set (i.e. their intersection is reducible). This is akin to only studying connected manifolds: some of the theory is nicer, but two connected submanifolds of $\mathbf{R}^n$ may intersect in a disconnected manifold.

There's a philosophical question lying in here: what makes a theorem interesting? Is it its statement, or its proof? This has practical applications to paper submission. Some people think it's only the statement that matters, but this is untrue; the proof of Theorem 14.1 will illustrate an awesome method called Noetherian induction.

Proof of Theorem 14.1. First, it will be shown that (1) $\Longrightarrow$ (2). Given that $X = Z_1 \cup \cdots \cup Z_n$ with the Z_i irreducible closed sets, one can clearly reduce to the irredundant case by throwing out the sets that are contained within the union of the others.

But what about uniqueness? Let $Z_1 \cup \cdots \cup Z_n = X = Z_1' \cup \cdots \cup Z_m'$ be two irredundant decompositions; then, we want to show that $n = m$ and $\{Z_i\}$ is a rearrangement of $\{Z_j'\}$.[40] In fact, it's sufficient to show that $Z_1 = Z_j'$ for some j, so that the rest of the theorem follows by induction.

Z_1 is irreducible, but it's a finite union of closed sets:

$$Z_1 = Z_1 \cap X = \bigcup_j (Z_1 \cap Z_j').$$

Thus, $Z_1 = Z_1 \cap Z_{j_0}' \subseteq Z_{j_0}'$ for some j_0. But then, play the same game again to show that $Z_1 \subset Z_{j_0}' \subset Z_i$ for some i, so $i = 1$ by the irredundancy condition, and thus $Z_1 = Z_{j_0}'$.

Remark. This show that for any irreducible closed set $Z \subset X$, there's an i such that $Z \subset Z_i$. The Z_i are in some sense the biggest irreducible closed sets, akin to the connected components of a manifold.

Digression. Heres an interesting proof that $\mathbf{Z}$ has infinitely many primes. Consider $\mathbf{Z}[\sqrt{-5}]$, which is not a UFD, e.g. $(2)(3) = (1+\sqrt{-5})(1-\sqrt{-5})$. Thus, there are infinitely many primes in $\mathbf{Z}[\sqrt{-5}]$, but they lift to $\mathbf{Z}$, so there are infinitely many primes in $\mathbf{Z}$. This proof is, oddly enough, not circular — commutative algebra doesn't depend on $\mathbf{Z}$ being a PID!

Back to the proof. For existence of a factorization in $\mathbf{Z}$, one can just keep factoring, and the numbers get smaller, forcing the process to terminate. Here, we wil prove that the nonempty closed subsets $Z \subset X$ are finite unions of irreducible closed subsets. The principle of Noetherian induction, which is *very* useful in algebraic geometry, uses the descending chain condition to get a "minimal counterexample," and exploits this minimality to obtain a contradiction.[41]

Suppose there exists a nonempty closed set $Z \subset X$ that is not such a finite union. Therefore, it cannot be irreducible, or $Z = \bigcup_{i=1}^{1} Z$ is such a finite union, and thus $Z = Z_1 \cup Z_2$, where both are nonempty, proper closed subsets of Z. One of these, without loss of generality Z_1, must also not be a union of finite closed subsets, so $Z \supsetneqq Z_1 \supsetneqq Z_2$ is a chain of counterexamples. But this violates the descending chain condition.[42] $\boxtimes$

These sorts of arguments come up a lot in algebraic geometry. The key is to generalize, e.g. to all closed sets, and the exploit minimality.

Excellent, but what does this tell us about affine algebraic sets?

Claim. Let A be a nonzero, finitely generated k-algebra, where k is an algebraically closed field. Then, for any proper ideal J:

- the set of prime ideals containing J has finitely many elements $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ under inclusion,
- all prime ideals $\mathfrak{p}$ containing J contain one, and
- $\operatorname{rad}(J) = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$.

---

[40] Again, this should be reminiscent of unique factorization of elements of $\mathbf{Z}$.

[41] This is the geometric analogue to the well-ordered property of $\mathbf{Z}$; in number theory, there are a lot of proofs with minimal counterexamples.

[42] Alternatively, consider the set of nonempty closed $Z \subset X$ that violate the property of interest. If this set is nonempty, then as above it contains a Z with $Z = Z_1 \cup Z_2$ for nonempty $Z_1, Z_2 \subsetneqq Z$. But by the minimality of Z, each Z_i has the property as well, so so does Z.

Proof. Since $\mathfrak{p} \supset J$ iff $\mathfrak{p} \supset \operatorname{rad}(J)$, then it's possible to assume J is radical, and thus lift inot $K[X_1, \ldots, X_n]$. This is because A is finitely generated, so there's a map $k[X_1, \ldots, X_n] \twoheadrightarrow A$, and under this lift, prime ideals and radical ideals are preserved. So without loss of generality, one can assume that $A = k[X_1, \ldots, X_n]$.

Thus, $\mathfrak{p} \supseteq J$, or equivalently, $\underline{Z}(\mathfrak{p}) \subseteq \underline{Z}(J) \neq \emptyset$, with $\underline{Z}(\mathfrak{p})$ an irreducible closed subset. Then, the assertion is exactly the irreducible decomposition of J into a finite union of irreducible closed subsets. ⊠

It's an amusing exercise to try to prove it directly, in terms of commutative algebra. But don't actually do that — it's so much better when you can actually see things!

Remark. Though the argument made was for finitely generated k-algebras, it ends up being true for any Noetherian ring, which will follow in HW6 from using the Zariski topology on $\operatorname{Spec} A$.

A variant of the claim expresses J as an intersection of primary ideals, which are *different* from prime ideals, even when J isn't radical.

Corollary 14.2. *Let k be an algebraically closed field, J be a radical ideal of $k[\underline{X}]$, and $Z = \underline{Z}(J)$. Then, the following are equivalent:*

(1) Z is finite (i.e. as a set of points).
(2) J is a finite intersection of maximal ideals.
(3) $\dim_k k[\underline{X}]/J$ is finite. In this case, there is a k-algebra isomorphism

$$k[\underline{X}]/J \xrightarrow{\sim} \prod_{z \in Z} k$$

given by $f \mapsto (f(z))$.

If J isn't radical, this is the geometric analogue to the structure theorem of local Artinian rings. Again, having schemes makes life a bit less tangled.

This corollary is in some sense the zero-dimensional case of the dimension theory of k-algebras.

Proof of Corollary 14.2.

- (1) $\Longrightarrow$ (2): The irreducible components of Z are points, which correspond to the maximal ideals.
- (2) $\Longrightarrow$ (3): If J is a finite intersection of maximal idelas, then $k[\underline{X}] \to k[\underline{X}]/\mathfrak{m}$ with kernel J as k-algebras, so $k[\underline{X}]/J \hookrightarrow \prod_{i=1}^n k[\underline{X}]/\mathfrak{m}_i$. But by the Nullstellensatz, $k[\underline{X}]/\mathfrak{m} \cong k$, so this is finite-dimensional over k.
- For (3) $\Longrightarrow$ (1), we want the irreducible components of Z to be points, i.e. every prime ideal $\mathfrak{p} \supset J$ is maximal. Well, $k[\underline{X}]/\mathfrak{p}$ is a domain, so $k[\underline{X}]/\mathfrak{p} \twoheadleftarrow k[\underline{X}]/J$, which is finite-dimensional over k, and any finite-dimensional domain over a field is also a field.

For the map, let $\{\mathfrak{m}_1, \ldots, \mathfrak{m}_\ell\}$ be the distinct maximal ideals containing J. Then, $\mathfrak{m}_i + \mathfrak{m}_j = (1)$ when $i \neq j$, so by the Chinese Remainder Theorem,

$$k[\underline{X}]/J = k[\underline{X}]/\bigcap_i \mathfrak{m}_i \xrightarrow{\sim} \prod_i k[\underline{X}]/\mathfrak{m}_i,$$

but by the Nullstellensatz, this is just $f \mapsto (f(z)) \in \prod_{z \in Z} k$. ⊠

Once again, direct proofs exist (c.f. Atiyah-McDonald, chapter 8), but they're not as nice.

15. Polynomial Maps: 2/7/14

Suppose k is algebraically closed and $F : k^m \to k^n$ is a "polynomial map," i.e. $\underline{x} = (x_1, \ldots, x_n) \mapsto (F_1(\underline{x}), \cdots F_n(\underline{x}))$ with each $F_j \in k[X_1, \ldots, X_n]$. Since k is infinite, the the set map F determines $F_1, \ldots, F_n \in k[X_1, \ldots, X_n]$.

This is analogous to an idea in differential geometry: that if $M \xrightarrow{F} N$ is C^∞, it gives a map of $\mathbf{R}$-algebras $F^* : C^\infty(N) \to C^\infty(M)$ sending $f \mapsto f \circ F$. In practice, viewing this as a map of $\mathbf{R}$-algebras isn't all that productive, but it makes the analogy snazzier.

In the same way, one can compose polynomials $f \in k[Y_1, \ldots, Y_n]$ with the polynomial map F: $F^*(f)$ is given by $k^m \xrightarrow{F} k^n \xrightarrow{f} k$. This sends $(x_1, \ldots, x_m) \mapsto f(F_1(\underline{x}), \ldots, F_n(\underline{x}))$. For example, $F^*(Y_3) = Y_3 \circ F = F_3$. Thus, the pullback is a k-algebra map $k[X_1, \ldots, X_m] \xleftarrow{F} k[Y_1, \ldots, Y_n]$, uniquely determined by $Y_j \mapsto F_j(\underline{X})$. It's also the case that all k-algebra maps $k[\underline{Y}] \to k[\underline{X}]$ can be given in this way for varying F.

But we want to restrict to the affine algebraic sets $\underline{Z}(J) \subset k^m$, so to speak, and $\underline{Z}(J') \subset k^n$, where $J \subset k[\underline{X}]$ and $J' \subset k[\underline{Y}]$ are radical. When does $F(\underline{Z}(J)) \subseteq \underline{Z}(J')$? This views maps between $\underline{Z}(J)$ and $\underline{Z}(J')$ pretty extrinsically, much like defining smooth maps between submanifolds as those that locally extend to Euclidean space. It's far from ideal, but in this situation isn't easy to avoid.

Claim. $F(\underline{Z}(J)) \subset \underline{Z}(J')$ iff $F^* : k[Y_1, \ldots, Y_n] \to k[X_1, \ldots, X_n]$ carries J' into J. In such cases, the following diagram commutes,

$$\begin{tikzcd} k[\underline{Y}]/J' \arrow[r, "F^*"] \arrow[d, hook, "\iota"] & k[\underline{X}]/J \arrow[d, hook] \\ \mathrm{Func}(\underline{Z}(J'), k) \arrow[r, "F\circ-"'] & \mathrm{Func}(\underline{Z}(J), k) \end{tikzcd} \tag{1}$$

where $F^* : k[\underline{Y}]/J' \to k[\underline{X}]/J$ is induced from the fact that J' is carried into J, and the inclusion ι uses the fact that $\underline{I}(\underline{Z}(J')) = J'$.

Here, $k[\underline{Y}]/J'$ is termed the coordinate ring of $\underline{Z}(J) \subset k^n$. The upshot is that this k-algebra map on the coordinate rings arises from the geometric map $F : \underline{Z}(J) \to \underline{Z}(J')$. Since the open sets are gigantic, one thinks globally; the Zariski topology is like a huge, somewhat imprecise pencil, so this is still acting locally, in some sense.

Proof. The proof is basically the Nullstellensatz, because we don't have anything else.

$F(\underline{Z}(J)) \subset \underline{Z}(J')$ is equivalent to saying that for every $z \in \underline{Z}(J)$ and $\varphi \in J'$, $\varphi(F(z)) = 0$, which is therefore equivalent to $F^*\varphi(z) = 0$. That is, for all $\varphi \in J'$, $F^*\varphi \in \underline{I}(\underline{Z}(J))$. But the Nullstellensatz says that's just J. Thus, this is equivalent to $F^*(J') = J$.

So we see that (1) commutes, and composition with $F_0 : \underline{Z}(J') \to \underline{Z}(J)$ induces the k-algebra map $k[\underline{Y}]/J \xrightarrow{F_0^*} k[\underline{X}]/J$ arising from F^*. Moreover, it's clear that any k-algebra map must arise in this way (where do the Y_i go?), and F_0 is uniquely determined from F_0^*, because if $\mathfrak{m}_x$ denotes the maximal ideal uniquely determined by x, then $\mathfrak{m}_{F_0(z)} = (F_0^*)^{-1}(\mathfrak{m}_z)$, and the preimage of a maixmal idea in this context is maximal. ⊠

This formula is a nice consequence of the formula on the whole affine space, and now we don't need to muck around with the ideals as much.

Digression. Needless to say, this is totally false over $\mathbf{R}$. It's disorienting, because that would seem like a better place to work, but the Nulstellensatz doesn't work, since $\mathbf{R}$ isn't algebraically closed. This is a bit disorienting, because $\mathbf{R}$ would seem like a better place to work.

There are some interesting results in real algebraic geometry; the following fact is already striking.

Fact. A field has an ordered structure iff -1 isn't a sum of squares.

Definition. A real closed field is an ordered field with no ordered algebraic extensions.

This is sort of the obvious notion. Good examples include $\mathbf{R}$, or the field of real algebraic numbers.

Theorem 15.1 (Artin & Schreier)**.** *The algebraic closure of a real closed field is given by adjoining $\sqrt{-1}$, and if k is a field such that $\overline{k}/k$ is finite, but nontrivial, then k is a real closed field.*

The proof is in Lang... somewhere.

Real algebraic geometry isn't a huge field,[43] and there's a real Nullstellensatz, which is uglier and involves sums of squares and the like. However, there are interesting ties to model theory and logic.

An excellent reference for real algebraic geometry is *Real Algebraic Geometry*, by Bochnak, Coste, and Roy. The professor strongly recommends reading the introduction, which is really fantastic (e.g., it mentions the remarkable fact that every compact smooth manifolds is diffeomorphic to a non-singular real algebraic set).

To state the real Nullstellensatz (Theorem 4.1.4 of that book), which incredibly was only proved in the 1970's (according to the introduction), one needs the notion of "real" ideal replacing that of "radical" ideal.

Definition. For a real closed field R, an ideal $J \subset R[X_1, \ldots, X_n]$ is called real if for any $f_1, \ldots, f_m$ satisfying $\sum (f_j)^2 \in J$ we always have $f_j \in J$ for all j.

Example 15.1. The ur-example is: if $S \subseteq \mathbf{R}^n$, then the ideal $\underline{I}(S)$ of elements $f \in \mathbf{R}[X_1, ..., X_n]$ vanishing on S is real.

Theorem 15.2 (Real Nullstellensatz)**.** *An ideal $J \subset R[X_1, ..., X_n]$ is real iff $\underline{I}(\underline{Z}(J)) = J$, where $\underline{Z}(J)$ is taken as its zero locus in $\mathbf{R}^n$.*

[43] No pun intended.

The proof rests on something called the Artin-Lang Homomorphism Theorem (Theorem 4.1.2 in that book) which roughly replaces the role of the weak Nullstellensatz in the proof of the usual Nullstellensatz.

There's also a notion of a "real spectrum" of a commutative ring in Chapter 7 of that book.

One should also note that in the theory of schemes, one can make sense of "algebraic geometry" over any field or ring whatsoever, such as over the field **R** of real numbers. But schemes over the field **R** are an entirely different beast from the objects one studies in real algebraic geometry over **R**.

So now we can say that a polynomial map between affine algebraic sets $\underline{Z}(J) \to \underline{Z}(J')$ is a map induced by a polynomial map $k^m \xrightarrow{F} k^n$. This seems super extrinsic, but the above discussion (ignoring the digression) shows that, in a precise sense, this is the same thing as a k-algebra map $k[\underline{X}]/J \leftarrow k[\underline{Y}]/J'$, which is reasonably intrinsic. Recall that $\underline{Z}(J) = \operatorname{MaxSpec}(k[\underline{X}]/J)$ (which is a finitely generated reduced k-algebra), so this is now intrinsic to the k-algebra without reference to the ambient k^n. The geometric notion of a polynomial map now has more geometric intuition.

Example 15.2.

(1) It's always good to think about hypersurfaces, e.g. $h(X,Y,Z) = 0 \subset k^3$ for some square-free polynomial h. Take $(X,Y,Z) \mapsto (X,Y)$, i.e. $F_1(X,Y,Z) = X$ and $F_2(X,Y,Z) = Y$, which projects from the graph down to the first two components. Then, the reverse map is $k[u,v] \to k[X,Y,Z]/(h)$, with $u \mapsto F_1 = X$ and $v \mapsto F_2 = y$.

(2) Consider $\{y^2 = x^3\} \subset k^2$, graphed in Figure 2, left. Send $F : t \mapsto (t^2, t^3)$; then, the induced map backwards sends $F^* : k[X,Y]/(Y^2 - X^3) \to k[T]$, with $X \mapsto F_1 = T^2$ and $Y \mapsto F_2 = T^3$. One can check this is an isomorphism onto the k-subalgebra $k[T^2, T^3]$ (i.e. things with a vanishing linear term).

(3) Jazzing it up a bit, consider $Z = \{u^2 = v(u+1)\}$, which is in some sense the curve $v = u^2/(u+1)$, graphed in Figure 2, right. We want to think about the projections $p_1 : (u,v) \mapsto v$ and $p_2 : (u,v) \mapsto u$, onto the u- or v-axes. Interestingly, $p_2^* : k[v] \to k[u,v]/(u^2 - v(u+1))$ is module-finite, because u satisfies a monic over v, but this is not true in the other direction, and therefore $p_1^* : k[u] \to k[u,v]/(u^2 - v(u+1))$ isn't module-finite (look at $(u+1)$-powers in the denominator). The consequence is that if v is bounded on some set, then u is bounded on the image of that set, but this is not true in the other direction.

Another way of thinking of this is asymptotically: projection to the v-axis is nice, two-to-one, and has bounded preimage (if the image is bounded), and it's yet nicer in **C**. But for u, there are asymptotes, and this doesn't hold. The important point is that algebraic properties of the ring extension have geometric meaning, so we get this blowup problem.

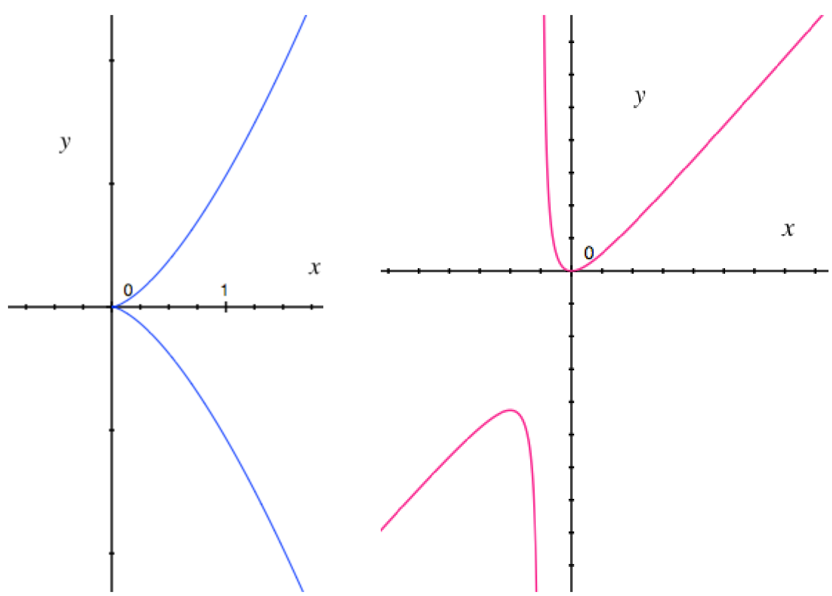


FIGURE 2. Left: the curve $y^2 = x^3$, corresponding to Example 15.2, part (2). Right: the curve $v = u^2/(u+1)$, corresponding to part (3).

(4) Consider $\mathrm{SL}_n(k) = \{\det(X_{ij}) = 1\} \subset \mathrm{Mat}_{n\times n}(k)$. Think about multiplication and inversion in $\mathrm{SL}_n(k)$, where $\mathrm{Mat}_n(k) \times \mathrm{Mat}_n(k)$ is the affine space, also $A = k[X_{ij}, Y_{ij}]/(\det(X_{ij}) - 1, \det(Y_{ij}) - 1)$. The map sends

$$(X_{ij}), (Y_{ij}) \longmapsto \sum_k X_{ik} Y_{kj},$$

and so the reverse map goes from $k[\underline{X}]/(\det(Z) - 1) \to A$.

Similarly, for inversion $\mathrm{SL}_n \to \mathrm{SL}_n$, X_{ij} is mapped to some stuff with minors. The point is, all of this stuff comes from polynomial maps, which is why some formulas, e.g. Cramer's Rule, work.

Remark. Just as in differential geometry, if $Z \xrightarrow{F_1} Z' \xrightarrow{F_2} Z''$, then $(F_2 \circ F_1)^* = F_1^* \circ F_2^*$, and $\mathrm{id}^* = \mathrm{id}$.

Now, what if A is a more general commutative ring? Then, we have $\mathrm{Spec}(A)$, and a ring map $A \xrightarrow{\varphi} B$ induces a map $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$, sending $\mathfrak{q} \mapsto \varphi^{-1}(\mathfrak{q})$, akin to $\mathfrak{m}_{F_0(z)} = (F_0^*)^{-1}(\mathfrak{m}_z)$ before.

Definition. Now, we can define the Zariski topology over any ring A, by taking the closed sets to be $V(I) = \{\mathfrak{p} \supset I\}$ for all ideals $I \subset J$.

We've already checked that this satisfies the properties for a topology, and the map $\mathfrak{q} \mapsto \varphi^{-1}(\mathfrak{q})$ is continuous. Furthermore, it's not hard to see that $V(I) = V(\operatorname{rad} I)$.

The analogy is, we can't do calculus over $\mathbf{Q}$, but at least it's dense in $\mathbf{R}$. Similarly, classical algebraic geometry worked with MaxSpec for sixty years without running into a problem.

Next time, we'll discuss how the topology of $\mathrm{Spec}(A)$ relates to properties of ideals of A, all motivated by the classical case.

16. Integral Ring Maps: 2/10/14

The polynomial map outlined in the previous lecture was defined over affine algebraic sets and such, but for more general rings, it'll be more useful to have $\mathrm{Spec}(A)$ rather than $\mathrm{MaxSpec}(A)$. For example, if R is local, $\mathrm{MaxSpec}(R) \subset \mathrm{Spec}(R)$ is the unique closed point, since the closure of $\mathfrak{p}$ is $V(\mathfrak{p}) = \{\mathfrak{q} \text{ prime} : \mathfrak{q} \supset \mathfrak{p}\}$. Thus, if the ring is huge, there will be lots of ideals, e.g. $\mathbf{C}[\![X, Y, Z]\!]$, or $\mathbf{C}[X, Y, Z]_{(X,Y,Z)}$.

The Zariski topology on $\mathrm{Spec}(A)$ has closed sets $V(I) - \{\mathfrak{p} \supset I\} = V(\operatorname{rad} I)$, but since $\operatorname{rad}(I)$ is the intersection of the prime ideals containing I (proved on HW6), then it can sort of be reconstructed from the topology. For radical I and J, $V(I) \subseteq V(J)$ iff $I \supseteq J$ (read straight from the definition); no Nullstellensatz is necessary, because we're not restricted to maximal ideals.

Spec is a bit more abstract, but these ways to visualize it do work.

Example 16.1. If $I \subset A$ is an ideal of A, then $A \twoheadrightarrow A/I$, and therefore $\mathrm{Spec}(A/I) \hookrightarrow \mathrm{Spec}(A)$ is a homeomorphism onto $V(I)$, found by unraveling the definition (containments and stuff); in particular, every closed set is Spec of something (though $\mathrm{Spec}(A/I) = \mathrm{Spec}(A/I^2) = \mathrm{Spec}(A/\operatorname{rad}(I))$, so just the topological space is insufficient to recover I).

Additionally, a base of opens is given by $X_\alpha = X - V((\alpha))$, so $\{X_\alpha\}_{\alpha \in I}$ covers $X - V(I)$. This is sort of like using balls in a manifold — it's sufficient for local coordinates. These X_α are called basic affine opens, because $A \to A_\alpha$ induces $\mathrm{Spec}(A_\alpha) \to \mathrm{Spec}(A)$, which is a homeomorphism onto X_α. It's useful to know that this open set, with its topologu, is the Spec of a ring, and the complement of a hypersurface (though it isn't uniquely determined, which makes life kind of hairier when we try to define sheaves of functions on stuff).

Integral Ring Maps. In topology, these are called covering spaces, e.g. $z \mapsto z^2$, $\mathbf{C}^\times \to \mathbf{C}^\times$, where locally, every point has two (or five, or some fixed number) preimages, with some continuity conditions, etc. But sometimes, there are bad points (e.g. 0 for $z \mapsto z^2$). The algebraic technique to understand this is integrality, which is the ring-theoretic analogue of algebraicity.

Recall Figure 2, which has a depiction of $u^2 = v(u+1)$ (though over $\mathbf{R}$, while we really want to understand it over $\mathbf{C}$), so the projections are $\mathrm{pr}_1 : k^2 \to k$ sending $(u, v) \mapsto u$ and $\mathrm{pr}_2 : k^2 \to k$ sending $(u, v) \mapsto v$, and similarly can be defined from $k[u, v]$ to $k[u]$ or $k[v]$. However, pr_1 is bad at $u = 1$; if v is bounded, the curve is, but not so for u. This suggests pr_2 is proper in the topological sense, but pr_1 isn't. And these are ring extensions satisfying some polynomials.

More generally, for a non-constant $f \in k[X, Y]$, $f = a_d(X)Y^d + \cdots + a_0(X)$ with the $\gcd(a_i) = 1$ (so that $\underline{Z}(f)$ has no vertical lines), and consider $k[X] \hookrightarrow k[X, Y]$. If a_d is non-constant, so that it has a root ρ, consider a zero of f away from $\underline{Z}(a_d)$:

$$y^d + \frac{a_{d-1}}{a_d} y^{d-1} + \cdots + \frac{a_0(x)}{a_d(x)} = 0.$$

Since the gcd is 1, then one of these terms must "blow up" as we get closer to $\underline{Z}(a_d)$; in this sense, one of the denominators must have a ρ.

Integrality will address this; it's an algebraic analogue to this geometric niceness condition.

Definition. A ring map $\varphi : A \to B$ is integral if for all $b \in B$, there exists a *monic* $f \in A[X]$ such that $f(b) = 0$ (i.e. $\varphi(f)(b) = 0$, technically). Then, one says b is integral over a.

Some authors require φ to be injective, but this makes life harder later on. Notice that for the field-theoretic case, algebraic relations can always be made monic (in one variable), and $k[X]$ is a PID, so there are minimal polynomials. But even if A and B are domains and φ is injective, the ideal theory of $A[X]$ is a mess, and there's generally not a good notion of minimal polynomial.

Thus, though minimality and algebraicity are related notions, they must be developed differently. Algebraicity isn't a good guide for minimality, as it's led by minimal polynomials.

If $b \in B$ is nilpotent, then by definition it's minimal over A. For example, if $A = \mathbf{Z}$ and $B = \mathbf{Q}[X]/(X^2)$, then every $n + qX$ with $n \in \mathbf{Z}$ and $q \in \mathbf{Q}$ is integral over $\mathbf{Z}$, since it comes in the form of a quadratic relation. These can be a little disorienting; one might expect integral elements of A to have A-valued coefficients, but not always.

Definition. Say that φ is (A)-finite if B is finitely generated as an A-module.

Topologically speaking, this is a generalization of the notion of a branched covering. Ambiguity with finite sets won't be an issue: we'll be clear which one we're talking about if both are in play.

In the field case, module-finiteness implies algebraicity. The same will be true here, but there's no nice dimensionality proof.

Example 16.2.

(1) If A is a field, then integrality over A is identical to algebraicity over A.

(2) If $A = \mathbf{Z}$ and $B = \mathbf{Q}$, then by the Rational Root theorem, the A-integral elements of B are exactly $\mathbf{Z}$. The same holds true for any UFD A, where $B = \mathrm{Frac}(A)$. This is why it's called 'integrality;' in nice cases, it corresponds to having no denominators.

(3) If $A = \mathbf{Z}$ and $B = \mathbf{Q}(\sqrt{3}) = \mathbf{Q}(\zeta_3)$, $b = \zeta_3 = (1 \pm \sqrt{3})/2$ is integral over A, because $(X^3 - 1)/(X - 1) = X^2 + X + 1 = f(X)$. But $b \notin \mathbf{Z}[\sqrt{-3}]$, and thus Euler's attempted proof of Fermat's Last Theorem was wrong. But inside $\mathbf{Z}[\zeta_3]$,[44] his proof does work! One of the great miracles of algebraic number theory is that the ring of integral elements over $\mathbf{Q}(\zeta_n)$ is $\mathbf{Z}[\zeta_n]$; it's generally hard to guess, and Kummer was just lucky.

(4) If A and B are domains and $A \hookrightarrow B$, then suppose $b \in B$ is algebraic over A. Then, we can sort-of clear denominators: $a_n b^n + \cdots + a_1 b + a_0 = 0$, so
$$(a_n b)^n + a_{n-1}(a_n b)^{n-1} + \cdots + a_0 a_n^{n-1} = 0,$$
and therefore $b = a_n b/a_n$ and $a_n b$ is integral. Generally, this isn't in A, but sometimes passing just into the integral case is nice.

(5) For a silly example, consider $A \twoheadrightarrow A/I = B$, because $X - a$ works if a is the preimage of b. But this is useful in a broader algebraic-geometric context.

Theorem 16.1. *For $\varphi : A \to B$ of rings and a $b \in B$, the following are equivalent.*

(1) b is integral over A.

(2) There exists an A-finite subalgebra $B' \subset B$ with $b \in B'$.

Corollary 16.2.

(1) If B is A-finite, then every $b \in B$ is integral (just take $B' = B$).

(2) The same proof that sums of algebraic elements are also algebraic works for integrality, and implies that $\{b \in B \mid b$ is integral over $A\}$ *is a subring and therefore an A-subalgebra of B.*

Definition. The A-subalgebra $\{b \in B \mid b \text{ is integral over } A\}$ is sometimes called the integral closure of A in B.

This is particularly cool if A is an integral domain and $B = \mathrm{Frac}(A)$. Whether the integral closure is finitely generated as an A-algebra is *very* subtle, even in the Noetherian case, even thought these are nice related (e.g. algebraic-geometric) properties. Thus, passing to an integral closure is pretty fundamental, and also concentrates singularities in places. But they're hard to calculate.[45] The definition is fairly exotic; how does one control the denominators?

[44] We'll see later that $\mathbf{Z}[\zeta_3] = \{b \in B \mid b \text{ is integral over } A\}$.

[45] These days, one uses a computer.

Proof of Theorem 16.1. For (1) $\implies$ (2), let $B' = A[b]$, which is the A-span of $\{1, b, \dots, b^{n-1}\}$ if $f(b) = 0$ for a monic $f \in A[X]$ of degree $n > 0$. Thus, B' is in fact an A-finite algebra.

For (2) $\implies$ (1), it's a bit more interesting. Rename B' as B (why not?), so $B = \sum_{i=1}^n Ab_i$ is finitely generated; this is just the span, as we have no linear independence result yet, since A isn't a field. Nonetheless, we're going to use matrices; inject $B \hookrightarrow \mathrm{End}_{A\text{-mod}}(B)$ (ok, well, not *quite* matrices) by sending $x \mapsto (m_x : y \mapsto xy)$. Then, $m_x(1) = x$, fine, and we want to show that m_b satisfies a characteristic polynomial. We would like to use the Cayley-Hamilton theorem, which we can't in some sense, but can in another sense.

Here's the idea. Take any $T \in \mathrm{End}_A(B)$; then, $T(b_j) = \sum_{i=1}^n a_{ij} b_i$, so consider the matrix $\mu_T = (a_{ij})$. This is totally not well-defined, but it is in $\mathrm{Mat}_n(A)$, and it does compute T. We don't want to go back and forth; we're just using it for computation.

If $\mu_{T'} = (a'_{ij})$, then $\mu_{T'}\mu_T = \mu_{T \circ T'}$, i.e. the product is one of the matrices that computes the map $T' \circ T$. Similarly, $a\mu_T + a'\mu_{T'} = \mu_{aT + a'T'}$ (this is an abuse of notation, but for every choice of μ_T and $\mu_{T'}$, the result is a matrix that computes $aT + a'T'$).

Thus, it suffices to show that every matrix $M \in \mathrm{Mat}_n(A)$ satisfies its characteristic polynomial $\chi_M(X) = \det(XM - I)$, which is monic in $A[X]$, a sort of generalized Cayley-Hamilton. In particular, we can reduce to the field case: it's enough to treat the universal case in n^2 variables, which is therefore in a domain, so it sits in its field of fractions.[46] $\boxtimes$

This method is useful in other places in commutative algebra, even if one could use Nakayama's lemma in this specific case.

17. Integral Closure: 2/12/14

There are two key cases of integral ring extensions, though one subsumes the other.

(1) If A is a domain and $F = \mathrm{Frac}(A)$, then one has $\widetilde{A} = \{x \in F \mid x \text{ is integral over } A\}$. Then, $\mathrm{Frac}(\widetilde{A}) = F$, and (as we'll see later today) $\widetilde{\widetilde{A}} = \widetilde{A}$; it's transitive, just like algebraicity. When $\widetilde{A} = A$, one says A is integrally closed, or normal.

(2) Let A be a normal domain, e.g. $\mathbf{Z}$ or $k[X, Y]$, and let F' be a finite extension of $F = \mathrm{Frac}(A)$. Then, $A' = \{x \in F' \mid x \text{ is integral over } A\}$ is called the integral closure of A in F'. In the case $A = \mathbf{Z}$, this is denoted $\mathscr{O}_{F'}$, the ring of integers of F'; in general, this is also called the normalization of A in F'. In this case, $A' \cap F = A$, because A is normal, and $\mathrm{Frac}(A') = F'$, which will come up later. Once again, the difference between integrality and algebraicity is due to denominators: there's basically a little bit of denominator chasing.

It's especially natural to ask, particularly in the case $A = \mathbf{Z}$, whether the above constructions are A-finite. These are important, but delicate problems (though for nice rings, such as $\mathscr{O}_F$, this is true, but hard to prove), and (1) is especially subtle. How should one universally bound denominators?

Let's start with some basic properties of integral closures and ring extensions. Let A be a domain and $F = \mathrm{Frac}(A)$. Lt A' be an extension of A with $\mathrm{Frac}(A') = F'$, which is finite over F.

Proposition 17.1. *Let $A \hookrightarrow B$ be a ring inclusion and $A' = \{b \in B \mid b$ is integral over $A\}$. Then,*

(1) A' is integrally closed in B, and

(2) if $B \hookrightarrow C$, then $B' = \{c \in C \mid c$ is integral over $A'\}$ is the integral closure of A in C.

Remark. Let $A = \mathbf{Z}$, $B = K$ and $C = K'$, so that the following diagram is satisfied.

$$\begin{tikzcd}
\mathscr{O}_{K'} \arrow[r, hook] \arrow[d, dash] & K' \arrow[d, dash] \\
\mathscr{O}_K \arrow[r, hook] \arrow[d, dash] & K \arrow[d, dash] \\
\mathbf{Z} \arrow[r, hook] & \mathbf{Q}
\end{tikzcd}$$

Then, this proposition says that $\mathscr{O}_{K'}$ is the integral closure of $\mathscr{O}_K$ in K'; these constructions sit well relative to each other, which is important for number theory. However, $\mathscr{O}_K$ and $\mathscr{O}_{K'}$ are both free over $\mathbf{Z}$, yet $\mathscr{O}_{K'}$ might not be free over $\mathscr{O}_K$. The point is, integrality is transitive, just like algebraicity.

[46] This is discussed in greater depth in a handout at: `http://math.stanford.edu/~conrad/210BPage/handouts/cayleyhamilton.pdf`.

Proof of Proposition 17.1. (2) implies (1) for suitable notation: use A' in the place of B and B in the place of C; then, $A \hookrightarrow A' \hookrightarrow B$. Thus, we'll focus on (2).

Ok, given B' over A' over A, we want to show that any $b' \in B'$ is integral over A, given that it was integral over A'. This is the same idea as algebraicity, with some thought to monicity. Well, $(b')^n + a'_{n-1}(b')^{n-1} + \cdots + a'_0 = 0$ for some $a'_j \in A'$, and think about $A[a'_0, \dots, a'_{n-1}, b'] \subset C$, which is an A-subalgebra. Then, it's enough to show that this is module-finite, as mentioned last time. But, $A[a'_0, \dots, a'_{n-1}]$ is module-finite over A, and $A[a'_0, \dots, a'_{n-1}][b]$ is module-finite over $A[a'_0, \dots, a'_{n-1}]$, so we're good. $\boxtimes$

Now for some denominator-chasing and localization.

Proposition 17.2.

(1) *For a multiplicative set $S \subset A$ and with $A \subset A' \subset B$ as above, integrality commutes with localization: $S^{-1}A' = (S^{-1}A)'$ (i.e. $\{x \in S^{-1}B \mid x$ is integral over $S^{-1}A\}$) in $S^{-1}B$.*

(2) *If A is a domain, then the following are equivalent:*
- *A is normal.*
- *$A_\mathfrak{m}$ is normal for all maximal ideals $\mathfrak{m}$ of A.*
- *$A_\mathfrak{p}$ is normal for all prime ideals $\mathfrak{p}$ of A.*[47]

Remark. In (1), if A is a domain and $B = \mathrm{Frac}(A) = F$, then suppose $0 \notin S$, Then, $S^{-1}(\widetilde{A}) = \widetilde{S^{-1}A}$ in F. As a special case, if A is integrally closed and $0 \notin S$, then $S^{-1}A$ is also integrally closed. This is related to singularities of algebraic curves, as we shall see.

Proof of Proposition 17.2. For part (1), we know that localization preserves injections, so $S^{-1}A \subset S^{-1}B$. First, we need to show that $S^{-1}B$ is integral over $S^{-1}A$: for $s \in S$, $a' \in A'$, we have that $(a')^n + a_{n-1}(a')^{n-1} + \cdots + a_0 = 0$ in B, and therefore
$$\left(\frac{a'}{s}\right)^n + \frac{a_{n-1}}{s}\left(\frac{a'}{s}\right)^{n-1} + \cdots + \frac{a_0}{s^n} = 0$$
in $S^{-1}B$, but the coefficient are in $S^{-1}A \subset S^{-1}B$, so we're good.

Conversely, suppose that $b/s \in S^{-1}B$ is integral over $S^{-1}A$. Then. the goal is to write it as a'/t for some $a' \in A$ and $t \in S$ such that $b/s = a'/t$. We have the monic relation
$$\left(\frac{b}{s}\right)^n + \frac{a_{n-1}}{s'}\left(\frac{b}{s}\right)^{n-1} + \cdots + \frac{a_0}{s'} = 0$$
in $S^{-1}B$ fo $a_i \in A$ and $s' \in S$. Thus, in $S^{-1}B$, which is still the wrong ring,
$$(s'b)^n + (sa_{n-1})(s'b)^{n-1} + \cdots + (s')^{n-1}s^n a_0 = 0.$$
Thus, there exists an $s'' \in S$ such that
$$s''((s'b)^n + (sa_{n-1})(s'b)^{n-1} + \cdots + (s')^{n-1}s^n a_0) = 0.$$
Multiply by $(s'')^{n-1}$ and let the dust settle; the conclusion is that $s''s'b \in A'$. Then, let $a' = s's''b$ and $t = s's''s$, so that $a' \in A'$, $t \in S$, and $a/s = b/t$.

Then, part (2) in the forward direction (A normal implies $A_\mathfrak{m}$ normal) follows by the previous remark, so suppose that all of the $A_\mathfrak{m}$ are normal, with fraction field $F = \mathrm{Frac}(A)$. Consider $A \subset \widetilde{A}$ in F; we want this to be equality. View these as A-modules — then, it's equivalent to checking after localizing at $\mathfrak{m}$, so from the first part, $(\widetilde{A})_\mathfrak{m} = \widetilde{(A_\mathfrak{m})}$. $\boxtimes$

Remark. One of the problems with normalization is that it satisfies a very weak mapping property (i.e. functoriality). Using domains and injections, it is possible to show that for every integrally closed domain B and every $\varphi : A \hookrightarrow B$, there exists a unique $\widetilde{\varphi} : \widetilde{A} \hookrightarrow B$ such that the folowing diagram commutes:
$$\begin{tikzcd} A \arrow[r, hook, "i"] \arrow[dr, hook, "\varphi"'] & \widetilde{A} \arrow[r, hook] \arrow[d, hook, "\widetilde{\varphi}"] & \mathrm{Frac}(A) \\ & B. & \end{tikzcd}$$

[47]It's important to have both the result with the prime ideals, which is more general, and the result with the maximal ideals, which is the classical algebraic geometry case, with points one can more easily see.

(Here, i is inclusion.) This corresponds to a diagram of maps of affine algebraic varieties with dense image (sometimes called dense maps): if $f : Y \to X$ is such a map, then there's a unique $\widetilde{f}$ such that the following diagram commutes.

$$\begin{tikzcd} Y \arrow[r, "f"] \arrow[d, "\widetilde{f}"'] & X \\ \widetilde{X} \arrow[ur] & \end{tikzcd}$$

Part of the issue is that we have $A \to A/\mathfrak{p}$ for a prime ideal $\mathfrak{p}$, but there is no corresponding map $\mathrm{Frac}(A) \to \mathrm{Frac}(A/\mathfrak{p})$.

Thus, if A fails to be integrally closed, there is some maximal ideal which also has this problem. This has geometric meaning; remember the curve $y^2 = x^3$? (See Figure 2 for a depiction.) Consider $t \mapsto (t^2, t^3)$; if $A = k[X,Y]/(Y^2 - X^3)$, then $A \hookrightarrow k[t]$ by $X \mapsto t^2$ and $Y \mapsto t^3$, which is easily seen to be an injection. Then, $t = Y/X$, so we have the same fraction field, and t is integral over A, because we have the relation $t^2 - X = 0$. But $k[t] = \widetilde{A} \neq A$, so there's some maximum ideal which has this problem too. It ends up being $\mathfrak{m} = (X, Y)$ (i.e. the origin, where the cusp is), the unique $\mathfrak{m} \in \mathrm{MaxSpec}(A)$ such that $A_{\mathfrak{m}}$ is not integrally closed.

Later, we will see that in dimension 1 (for a definition of dimension we'll provide later), normality is equivalent to smoothness. But this breaks down if the dimension is at least 2; for example, the cone $k[X,Y,Z]/(XY - Z^2)$ is normal, but not smooth at the origin.

In general, normality implies smoothness up to codimension at least 2; the converse isn't quite true, but it's a vague principle that's useful for guiding intuition. This relates to Serre's criterion for normality.

How does one calculate normalization? For example, we'll talk about the case $\mathscr{O}_K$ for $K = \mathbf{Q}(\sqrt{d})$ next time. $\mathbf{Q}(\zeta_n)$ is a bit more subtle (this is a standard thing to do in algebraic number theory), and $\mathbf{Q}(2^{1/n})$ even more so: it's usually, but not always, $\mathbf{Z}[2^{1/n}]$. For $\mathbf{Q}(\alpha)$, the ring of integers isn't always $\mathbf{Z}[\alpha]$, e.g. $K = \mathbf{Q}(\theta)$ where $\theta^3 + \theta^2 - 2\theta + 8 = 0$; this is irreducible (try mod $p = 3, 5$), but $\mathscr{O}_K \neq \mathbf{Z}[\alpha]$ for any α.

Roughly speaking, expressing $\mathbf{Z}[X_1, \dots, X_n] \twoheadrightarrow \mathscr{O}_K$ as a quotient is analogus to putting an algebraic curve inside $\mathbf{A}_k^{n+1}$, where $k = \mathbf{F}_q$; maybe this has more than q^{n+1} rational points, so sometimes it can't be embedded in there. It relates to how many prime ideals sit over a given prime, clarifying Dedekind's example.

Unlike in the case of algebraicity, the above discussion implies there's no primitive element theorem; it's more complicated.

18. Finiteness Properties of Integral Extensions: 2/14/14

Galois descent is how Galois theory is actually used in the real world; it's the first crucial example of how to extend a field and then go back down. There are beautiful analogues with topology beyond the scope of the class.

Theorem 18.1. *Let $A \subset F$ be an integrally closed Noetherian domain and F'/F be a finite extension of fields. If A' is the integral closure of A in F', then A' is A-finite.*

The converse isn't quite true, but counterexamples are few — and due to a theorem of Grothendieck, these don't really correspond to real-life examples, in some sense. Nagata found a ring whose integral closure is its own fraction field, even.

A more down-to-earth thing about the theorem is that the coordinate ring of an affine algebraic variety is often not integrally closed (e.g. if it self-intersects). Finiteness conditions such as this one are common later in algebraic geometry; the idea is to bound the denominators.

Proof of Theorem 18.1. Let e_j' be an F-basis for F', so that $F' = \bigoplus F e_j'$, and without loss of generality scale the e_j' so that they're all in $A' \subset F'$. Then, the goal is to find some nonzero $d \in A$ that's a multiple of all the denominators of elements of A with respect to $\{e_1', \dots, e_n'\}$. In other words, we want to show that $d \cdot A' \subset \bigoplus A \cdot e_j'$; this would imply $A' \cong d \cdot A'$ is finitely generated, because the sum of the $A \cdot e_j'$ is finitely generated Noetherian.

Consider the trace form $B = \mathrm{Tr}_{F'/F} : F' \times F' \to F$, sending $(x', y') \mapsto \mathrm{Tr}_{F'/F}(x'y')$. Since F'/F is separable, this is a nondegenerate, F-bilinear form, and in particular, carries

$$A' \times A' \to \{z \in F \mid Z \text{ is integral over } A\} = A,$$

because A is integrally closed.

Let $\widetilde{F}'$ denote the Galois closure of F' and Σ be the set of embeddings $\sigma : F' \to \widetilde{F}'$ that preserve F. Thus,

$$\mathrm{Tr}_{F'/F}(z') = \sum_{\sigma \in \Sigma} \sigma(z'),$$

and therefore the trace preserves integrality.

Choose a typical element $x' = \sum c_j e'_j$ in A' (with the $c'_j \in F = \text{Frac}(A)$). Will we be able to control the denominators? Can we start taking pairings with B, akin to the same idea in Fourier analysis?

$$B(x, e'_i) = \sum_j c_j B(e'_j, e'_i) \in A,$$

so we get a fixed matrix:

$$(B(e'_j, e'_i)) \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} \in A^n.$$

$c_1, \dots, c_n \in F$, so this matrix, over A, is a map $F^n \to A^n$. Notice also that since B is nondegenerate, it has nonzero determinant d, so apply Cramer's formula. You get some messy stuff in A, but the point is that $(c_1, \dots, c_n) \in (1/d)A^n$, which is what was to be shown. ⊠

Corollary 18.2. *If $K/\mathbf{Q}$ is a finite extension, then $\mathcal{O}_K$ (the integral closure of $\mathbf{Z}$ in K) is a fintie free $\mathbf{Z}$-module of rank $[K : \mathbf{Q}]$.*

Proof. $\mathcal{O}_K$ is $\mathbf{Z}$-finite and torsion-free (since it's characteristic zero), and therefore free. Now, $\mathbf{Q} \otimes_{\mathbf{Z}} \mathcal{O}_K = K$ (i.e. everything in K is an algebraic integer divided by an integer), but this has $\mathbf{Q}$-dimension equal to the $\mathbf{Z}$-dimension of $\mathcal{O}_K$. ⊠

Wonderful! But how do you compute it? There will be some examples on the homework.

Remark. Kummer showed that if $K = \mathbf{Q}(\zeta_n)$, then $\mathcal{O}_K = \mathbf{Z}[\zeta_n]$. However, if $K = \mathbf{Q}(10^{1/3})$, then $\mathcal{O}_K \supsetneq \mathbf{Z}[10^{1/3}]$, ultimately because $10 \equiv 1 \pmod 9$. It's generated by $\beta = (1+10^{1/3}+(10^{1/3})^2)/3$, i.e. satisfying $\beta^3 - \beta^2 - 3\beta - 3 = 0$. This is not aways obvious.

For another example of how much cleverness might be necessary, when $K = \mathbf{Q}(2^{1/n})$, $\mathcal{O}_K = \mathbf{Z}[2^{1/n}]$ for $n < 1093$, and then fails. This has something to do with the fact that 1093 is a Wiefricht prime (so that $2^{p-1} \equiv 1\ (p^2)$, where $p = 1093$). There are only two known examples, though they were a real headache for people proving Fermat's last theorem.

Proposition 18.3. *Let $d \in \mathbf{Z} \setminus \{0, 1\}$ be square-free and $K = \mathbf{Q}(\sqrt{d})$. Then,*

$$\mathcal{O}_K = \begin{cases} \mathbf{Z}[\sqrt{d}], & d \equiv 2, 3 \quad (4) \\ \mathbf{Z}\left[\frac{1+\sqrt{d}}{4}\right], & d \equiv 1 \quad (4). \end{cases}$$

Thus, usually (two-thirds of the time), $\mathcal{O}_K = \mathbf{Z}[\sqrt{d}]$. In the remaining case, where $\alpha = (1 + \sqrt{d})/4$, it looks fractional but is actually integral: $\text{Tr}_{K/\mathbf{Q}}(\alpha) = 1$ and $N(\alpha) = (1 - d)/4$, so they're both integers. This is related to Euler's failure to prove Fermat's last theorem, which we discussed last tme: $\mathbf{Z}[\zeta_3] = (-1 + \sqrt{3})/2$, and $-3 \equiv 1 \bmod 4$.

Remark. We have $\mathcal{O}_K \supset \mathbf{Z} \oplus \mathbf{Z}[\sqrt{d}]$ for this quadratic extension, so $e'_1 = 1$ and $e'_2 = \sqrt{d}$. Thus,

$$(B(e'_i, e'_j)) = 2\begin{pmatrix} \text{Tr}(1) & \text{Tr}(d) \\ \text{Tr}(d) & \text{Tr}(d) \end{pmatrix},$$

so its determinant is $4d$. Thus, by the algorithm in the proof of Theorem 18.1, $\mathcal{O}_K \subseteq (1/4d)\mathbf{Z}[\sqrt{d}]$. Thus, the proof doesn't provide the best bound.

Proof of Proposition 18.3. Let $\alpha = a + b\sqrt{d} \in \mathcal{O}_K$ with $a, b \in \mathbf{Q}$. Then, $\text{Tr}(\alpha) = 2a \in \mathbf{Z}$, so $a = n$ or $a = n/2$ with n odd. Then, $N(\alpha) = a^2 - db^2 \in \mathbf{Z}$.

Case 1. If $a = n \in \mathbf{Z}$, then $n^2 - db^2 \in \mathbf{Z}$, so $db^2 \in \mathbf{Z}$. Since d is square-free, then $b \in \mathbf{Z}$ too (otherwise, we couldn't clear the denominators), so $\alpha \in \mathbf{Z}[\sqrt{d}]$.

Case 2. If $a = n/2$ for n odd, then $n^2/4 - db^2 \in \mathbf{Z}$; since n is odd, we can't clear the denominator. Thus, we need to have exactly $b = m/2$ for m and d both odd (we can't have extra because d is square-free). Thus, $n^2 0 dm^2 \equiv 0 \bmod 4$. Then, odd squares are all 1 mod 4, so $d \equiv 1 \bmod 4$. Thus, in this case,

$$\alpha = \frac{n}{2} + \frac{m}{2}\sqrt{d} = \Bigg(\underbrace{\frac{1}{2} + \frac{\sqrt{d}}{2}}_{\text{yields desired result}} \Bigg) + \Bigg(\underbrace{\frac{n-1}{2} + \frac{m-1}{2}\sqrt{d}}_{\text{in } \mathbf{Z}[\sqrt{d}]} \Bigg).$$ ⊠

Needless to say, this game doesn't work very well for cubic fields. It can be adapted to hyperelliptic curves, i.e. $k[X,Y]/(Y^2 - f(X))$, where f is square-free. What one winds up proving is that it's integrally closed, except in characteristic 2.

Anothr reasonable question: is $\mathscr{O}_K$ always a PID? Number theory would be so much simpler... there are plenty of counterexamples. Dedekind domains are a workaround for this, in fact. For example, if $K = \mathbf{Q}(\sqrt{-5})$, then $\mathscr{O}_K = \mathbf{Z}[\sqrt{-5}]$, and $6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ gives us two genuinely distinct factorizations. It takes a little more work to calculate the units and finish the proof, though.

Lemma 18.4. $\mathbf{Z}[\sqrt{-5}]^\times = \{\pm 1\}$.

Proof. If $a + b\sqrt{-5}$ with $a, b \in \mathbf{Z}$ is a unit, then $N(a + b\sqrt{-5}) \in \mathbf{Z}^\times$, so it's ± 1. Thus, $a^2 + 5b^2 = 1$, and therefore $a^2 = 1$ and $b^2 = 0$. ⊠

The above lemma can be generalized.

Thus, the factors we talked about above aren't obtained from each othr by scaling by ± 1; we must still show irreducibility, though. If $2 = \alpha\beta$, then $4 = N(\alpha)N(\beta)$, but this means $N(\alpha) = N(\beta) = 2$ (if α and β aren't units). However, if $a^2 + 5b^2 = 2$, then we have a bit of a problem. The same thing happens with 3 and with $6 = N(1 \pm \sqrt{-5})$.

What's really happening here? Later, ideal factorization in Dedekind domains will explain this example. In $\mathbf{Z}$, $6 \cdot 35 = 14 \cdot 15$ isn't a counterexample, but the real point is that in $\mathbf{Z}[\sqrt{-5}]$, the ideal (2) decomposes into products of non-principal ideals. This leads to different ways of stuffing them together.

Thus, $\mathbf{Z}[\sqrt{-5}]$ isn't a UFD, and also therefore not a PID. An explicit example of a non-principal ideal is $(2, 1+\sqrt{-5})$, which is really ugly to prove directly, unless you use norms, in which case it's really easy. Fine.

Here's anothr natural question; suppose K and K' over $\mathbf{Q}$ are linearly disjoint, meaning $L = K \otimes_{\mathbf{Q}} K'$ is a field, e.g. $K = \mathbf{Q}(\sqrt{-2})$ and $K' = \mathbf{Q}(\sqrt{-6})$. Then, by general nonsense with tensor products, $K \otimes_{\mathbf{Q}} K' = \mathbf{Q} \otimes_{\mathbf{Z}} (\mathscr{O}_K \otimes_{\mathbf{Z}} \mathscr{O}_{K'}) \hookleftarrow \mathscr{O}_K \otimes_{\mathbf{Z}} \mathscr{O}_{K'} \subseteq L$. Is this injection equality? Sometimes; it depends on something called the ramification theory of K and K'. Basically, products of smooth manifolds are smooth, but products of singularities can be even worse singularities. In the example with $\mathbf{Q}(\sqrt{-2})$ and $\mathbf{Q}(\sqrt{-6})$, equality doesn't hold, and $\mathscr{O}_L$ isn't even $\mathscr{O}_K$-free!

19. The Topology of Spec(A): 2/18/14

This week's lectures were given by Greg Brumfiel.

Let A be a commutative ring. The stuff having to do with Spec(A) is easier than some of what we've been doing, especially if you're familiar with the language of topology.

The closed sets of $X = \mathrm{Spec}(A)$ are $V(J) = \{\mathfrak{p} \supset J\}$. We can check the axioms of a topology:

- The union of two closed sets must remain closed: $V(I) \cup V(J) = V(IJ) = V(I \cap J)$, which is good (this is still an ideal).
- Arbitrary intersections of closed sets remain closed. This is true because

$$\bigcap V(J_\alpha) = V\Big(\sum J_\alpha\Big).$$

The basic opens are $X_\alpha = \{\mathfrak{p} \not\supset (\alpha)\}$ for $\alpha \in A$. We also have radicals: $V(I) \subset V(J)$ iff $\sqrt{I} \supset \sqrt{J}$ (here, $\sqrt{J} = \mathrm{rad}(J)$ is another common notation for the radical of an ideal).

To see why the X_α are a basis, any open set is of the form $X \setminus V(J)$ for some J, but

$$X \setminus V(J) = \bigcup_{\alpha \in J} X_\alpha.$$

Furthermore, these basic opens have some nice properties: if $a, b \in A$, then $X_a \cap X_b = X_{ab}$ (their product). Later, it will turn out to be useful that $X_{ab} = X_{a^n b^m}$, or more generally $X_a = X_{a^n}$.

Ring homomorphisms between commutative rings induce contravariant continuous maps on Spec; see the handout.[48]

Definition. A topological space is quasi-compact if every open covering has a finite subcovering.

In some branches of mathematics, this is taken as the definition of compactness; however, here, it is called quasi-compact, and a compact space is usually assumed to be Hausdorff.

Three things are immediate.

Proposition 19.1.

(0) X is quasi-compact.

[48] Located at `http://math.stanford.edu/~conrad/210BPage/handouts/spec.pdf`.

(1) *Each basic open X_α is quasi-compact.*[49]
(2) *If J is a finitely generated ideal, then $X \setminus V(J)$ is quasi-compact.*

Note that if A is Noetherian, then all of its ideals are finitely generated, so all open sets of Spec(A) are quasi-compact. This is pretty weird.

Since
$$X \setminus V(J) = \bigcup_{i=1}^{n} X_{a_i}$$
if $J = (a_1, \ldots, a_n)$, then (1) $\implies$ (2). Furthermore, (0) $\implies$ (1), because for all commutative A, $\operatorname{Spec}(A_a) = X_a$, where $A_a = A[1/a]$ is the localization. The points are nice, because primes are well-behaved in A_a, but the topological consideration requires some work.

Proof of Proposition 19.1. Let's start with (1). Suppose
$$X_a \subset \bigcup_\alpha U_\alpha = \bigcup X_{a_i},$$
since we're working in the relative topology. Then,
$$X \setminus X_a = V(a) \supset \bigcap V((a_i)),$$
i.e. $a \in \sqrt{(a_i)}$ for each i. This means that a has a relation in terms of only finitely many X_{a_i}, and therefore $X_a \subset \bigcup_{i=1}^n X_{a_i}$ is a finite subcover.

For (0), $X = X_1 = \bigcup_{i=1}^n X_{a_i}$, and therefore $\emptyset = \bigcap V((a_i))$. Thus, no primes contain all of the a_i, so $1 \in (a_1, \ldots, a_n)$, so 1 is a finite linear combination of the a_i (which is a subcovering); the radical goes away because $1^e = 1$. ⊠

Residue Fields. For a $\mathfrak{p} \in X$ (i.e. a prime idea of A), associate $k_\mathfrak{p}$, the fraction field of $A/\mathfrak{p}$ (since $A/\mathfrak{p}$ is an integral domain), i.e. $k_\mathfrak{p} = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$, because $\mathfrak{p}A_\mathfrak{p}$ is the maximal ideal of the local ring $A_\mathfrak{p}$. Thus, for each $a \in A$, there's a "function" $a(\mathfrak{p}) = a \bmod \mathfrak{p} \in k_\mathfrak{p}$, though the target varies, which is strange. It can happen that $a(\mathfrak{p}) = 0$ for all $\mathfrak{p} \in X$, i.e. $a \in \mathfrak{p}$ for all $\mathfrak{p}$, which is equivalent to a being nilpotent (i.e. $a \in \sqrt{0}$; $\sqrt{0}$ is sometimes called the nilradical). Since $\operatorname{Spec}(A) \cong \operatorname{Spec}(A/\sqrt{0})$, one might wonder why we don't always kill the nilradical, but it's sometimes useful in quotient rings.

For example, if k is algebraically closed and $A = k[x_1, \ldots, x_n]/I$, then the variety of I, $V(I) \subset k^n$ (that is, $\underline{Z}(I)$) can be viewed in MaxSpec(A), the set of maximal ideals, by the Nullstellensatz. If $f \in A$, then one can check that for a maximal ideal $\mathfrak{m}$, $f(\mathfrak{m})$ sends $\mathfrak{m} \mapsto (\gamma_1, \ldots, \gamma_n) \in k^n$, where $\mathfrak{m} = (x_1 - \gamma_1, \ldots, x_n - \gamma_n)$. This is an honest function: one really does get k-valued functions and stuff. It's a special case of the more general function for residue fields above.

As an example of where nilpotent elements tell you something, look at k^2 and the affine algebraic sets $V(y)$ and $V(y - x^2)$, as plotted in Figure 1, page 25. Geometrically, these two varieties intersect at the origin: $\{(0,0)\} = V(y) \cap V(y - x^2) = V((y) + (y - x^2))$. This is correct, but there's more information to be found in this construction. Modding out, $k[x,y]/(y - x^2) \cong k[x]/(x^2)$, an algebra of dimension 2 over k, which says something about the tangency of this intersection. This information is lost when one mods out by the nilradical.

Th application of these ideas and techniques to arbitrary rings, including those with nilpotent elements, rather than just to finitely generated k-algebras, is the seat of power of the modern presentation of algebraic geometry.

Recall that we had a notion of a closed set being irreducible if whenever $Z = Z_1 \cap Z_2$ for closed Z_1 and Z_2, then $Z = Z_1$ or $Z = Z_2$. This is silly in the normal geometrical context, after all, but in Spec(A), $Z = V(J)$ is irreducible iff $\sqrt{J}$ is a prime ideal.

Returning to the specific case where k is algebraically closed and $k^n = \operatorname{MaxSpec}(k[x_1, \ldots, x_n])$, the idea is that $V(\mathfrak{p})$ has lots of zeroes. The point $\mathfrak{p} \in \operatorname{Spec}(k[x_1, \ldots, x_n])$ is identified with the irreducible closed set $V(\mathfrak{p}) \subseteq k^n$. In some sense, you add one new point for each non-maximal ideal, but these points are called generic points. They sound kind of weird, but aren't unheard of in topology. Each set is a point, or a shadow of a point in MaxSpec…

Returning to our "function" above, if $\varphi \in k[x_1, \ldots, x_n]_\mathfrak{p}$, so that $\varphi = f/g$ for some $g \notin \mathfrak{p}$ (and therefore $g \neq 0$), then this is an honest function near $V(\mathfrak{p}) \subset k^n$. In some sense, this is the real locality of localization: it's a function in a local neighborhood. These can be used to characterize $\mathfrak{p}$; by the Nullstellensatz, if $\mathfrak{p}' \notin V(\mathfrak{p})$, then there's a function distinguishing $\mathfrak{p}'$ and $V(\mathfrak{p})$.

Returning to the general case, points $\mathfrak{p} \in \operatorname{Spec}(A)$ aren't necessarily closed; in fact, if $\mathfrak{p}$ is viewed as a prime, then its closure is $\overline{\{\mathfrak{p}\}} = \{\mathfrak{q} \supseteq \mathfrak{p}\}$ (which is a nice exercise). This implies the closed points are the maximal ideals.[50] The

[49] This is uncommon in most topological spaces.

[50] The special case has the property that every prime is the intersection of the maximal ideals that contain it. This is not true in general.

MaxSpec of any ring has closed points, but is still extremely far from being Hausdorff; for example, in Spec($k[T]$), the closed sets are the entire space and finite collections of points, so open sets have *huge* intersections.

Example 19.1.

- Spec($\mathbf{Z}$) has a bunch of points on a line, corresponding to the maximal ideals (2), (3), (5), (7), and so on. However, (0) is a generic point; every $\mathfrak{p} \in \overline{(0)}$, since $0 \in \mathfrak{p}$, and therefore (0) is dense.
  If $\mathfrak{p} \neq (0)$, then the residue field is just $\mathbf{Z}/\mathfrak{p}$; since $\mathfrak{p}$ is maximal, so there's no need for a field of fractions. For (0), one obtains $k_{(0)} = \mathbf{Q}$. For each $n \in \mathbf{Z}$, we get a point in each residue field: $n \mapsto n \bmod \mathfrak{p}$ or $n \mapsto n \in \mathbf{Q}$.
- For Spec($\mathbf{Q}[t]$), it looks similar, on a line, but with more points $(t-r)$ for every $r \in \mathbf{Q}$. However, it's really the complex line (or at least $\overline{\mathbf{Q}}$), because there are higher-degree irreducibles, and their maximal ideals are identified with their roots in $\mathbf{C}$.
  If you go back and look at the residue field construction, $(0) \to \mathbf{Q}(t)$ (the rational functions); for $r \in \mathbf{Q}$, the residue field of $(t-r)$ is just $\mathbf{Q}[t]/(t-r) \cong \mathbf{Q}$, sending $g \mapsto g(r)$. In the general case, where (f) is irreducible, $\mathbf{Q}[t]/((f(t))$, sending $g \mapsto g \bmod f$ allows one to see all finite algebraic extensions of $\mathbf{Q}$.
- Consider Spec($\mathbf{Z}[1/15]$): here, (0) is once again generic, and we have points corresponding to (2), (7), (11), (13), and so on: primes, but missing 3 and 5, which were killed by the localization. Here, the residue fields are $\mathbf{Z}/p$ or $\mathbf{Q}$ again, so $7/15 \mapsto 7(15^{-1} \bmod \mathfrak{p})$ or $7/15 \in \mathbf{Q}$.

20. The Going-Up and Going-Down Theorems: 2/19/14

Today's lecture was also by Greg Brumfiel.

The Going-Up and Going-Down Theorems are about integral extensions $A \xrightarrow{\varphi} B$ of commutative rings and the behavior of $\varphi^* : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ (given by $\mathfrak{q} \mapsto \varphi^{-1}(\mathfrak{q})$). This doesn't preserve maimal ideas (except in the classic case of affine rings over algebraically closed fields), e.g. $\mathbf{Z} \hookrightarrow \mathbf{Q}$, which is why the theory is over prime ideals in general, even though they have weird stuff such as generic points.

Example 20.1. Actually, this is more like a non-example.

Consider $A = k[x] \hookrightarrow k[x,y]/(xy-1) = B$, where k is algebraically closed. This is the real hyperbola $y = 1/x$. $A \hookrightarrow B$ isn't integral, because $B = k[x, 1/x]$, so it can't satisfy a monic relation (as a module, it's generated by $1/x$, $1/x^2$, and so forth; we can't multiply them together, since this is as a module, not a ring).

Thus, the reduced ring map $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ has some issues. We're basically localizing at x, so $\mathfrak{p} = (x) \in \mathrm{Spec}(A)$ has no preimage, and the image of φ^* isn't closed (these are ideals under localization; what gets sent to 0?).

These are all things that go right in the case of integral extensions, thanks to the Going-Up theorem.

Definition. If $\varphi : A \hookrightarrow B$ as rings, $\mathfrak{p} \in A$, and $\mathfrak{q} \in B$ are such that $\mathfrak{q} \cap A = \mathfrak{p}$, then $\mathfrak{q}$ is said to lie over (or be over) $\mathfrak{p}$.

Theorem 20.1 (Going-Up)**.** *Suppose $\varphi : A \hookrightarrow B$ is integral.*

(1) $\varphi^* : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is surjective.
(2) φ^* carries closed sets to closed sets: $\varphi^*(V(J)) = V(J \cap A)$.
(3) Given prime ideals $\mathfrak{p}_0 \subset \mathfrak{p}_1$ of A and a prime ideal $\mathfrak{q}_0 \subset B$, if $\mathfrak{q}_0$ is over $\mathfrak{p}_0$, then there exists a prime ideal $\mathfrak{q}_1$ of B such that $\mathfrak{q}_1 \supset \mathfrak{q}_0$ and $\mathfrak{q}_1$ lies over $\mathfrak{p}_1$.
(4) Suppose $\mathfrak{q} \subseteq \mathfrak{q}'$ and both $\mathfrak{q}$ and $\mathfrak{q}'$ lie over $\mathfrak{p}$; then, $\mathfrak{q} = \mathfrak{q}'$.

Part (3) can be thought of as ensuring that every prime lifts, preventing the scenario in Example 20.1, and (4) is a nice little uniqueness result. The "going-up" refers to part (3), though it could also refer to lifting prime ideals via the surjection $\mathrm{Spec}(B) \twoheadrightarrow \mathrm{Spec}(A)$, though I guess that's not what it refers to.

The key is the following lemma.

Lemma 20.2. *Suppose $A \hookrightarrow B$ is integral and $\mathfrak{q} \subset B$ is a prime ideal. Let $\mathfrak{p} = \mathfrak{q} \cap A$.*

(1) If $\mathfrak{p}$ is maximal, then $\mathfrak{q}$ is.
(2) If $\mathfrak{q}$ is maximal, then $\mathfrak{p}$ is.

Proof. (1) has almost nothing to do with integrality. Since $\mathfrak{p} = \mathfrak{q} \cap A$, then $A/\mathfrak{p} \hookrightarrow B/\mathfrak{q}$, but $A/\mathfrak{p}$ is a field and $B/\mathfrak{q}$ is a domain (since $\mathfrak{q}$ is prime) that is also an algebraic extension of a field (since $A \hookrightarrow B$ is integral; the monic polynomial doesn't go to 0 in the quotient). Thus, it too is a field: if $b \in B$ and $\overline{b} = b \bmod \mathfrak{q}$, then $A/\mathfrak{p}[\overline{b}]$ is a finitely generated $A/\mathfrak{p}$-algebra, and therefore must contain b^{-1}. Since $B\mathfrak{q}$ is a field, then $\mathfrak{q}$ is maximal.

In the other direction, to prove (2), we still have $A/\mathfrak{p} \hookrightarrow B/\mathfrak{q}$, but this time, $B/\mathfrak{q}$ is a field. Choose an $a \neq 0$ in $A/\mathfrak{p}$, so that $1/a$ exists in $B/\mathfrak{q}$. Therefore

$$0 = \left(\frac{1}{a}\right)^n + a_{n-1}\left(\frac{1}{a}\right)^{n-1} + \cdots + a_1\left(\frac{1}{a}\right) + a_0,$$

where the $a_i \in A/\mathfrak{p}$. When we clear the denominators, we see that $1 = ax$ for some $x \in A/\mathfrak{p}$, and therefore a is invertible mod $\mathfrak{p}$. Thus, $\mathfrak{p}$ is maximal. ⊠

Proof of Theorem 20.1. For part (1), pick a $\mathfrak{p} \subset A$ and localize: $A_\mathfrak{p} \hookrightarrow B_\mathfrak{p}$ is still integral,[51] because we saw that localization preserves integrality (and we also saw that it preserves injectivity back in 210A). Since $0 \in \mathfrak{p}$, then $B_\mathfrak{p} \neq (0)$, so there's a maximal ideal $\widehat{\mathfrak{q}} \subset B_\mathfrak{p}$. By Lemma 20.2, $\widehat{\mathfrak{p}} = A_\mathfrak{p} \cap \widehat{\mathfrak{q}}$ is maximal in $A_\mathfrak{p}$, and since $A_\mathfrak{p}$ is local, that's the only maximal ideal, so $\widehat{\mathfrak{p}} = \mathfrak{p}A_\mathfrak{p}$. Thus, we can get a preimage of $\mathfrak{p}$ by running around the following diagram.

$$\begin{tikzcd} A \arrow[r, hook] \arrow[d] & B \arrow[d, "\pi"] \\ A_\mathfrak{p} \arrow[r, hook] & B_\mathfrak{p} \end{tikzcd}$$

Specifically, since this diagram commutes, it still commutes once we take Spec of it and reverse all the arrows; in particular, $\pi^{-1}(\widehat{\mathfrak{q}})$ is the desired preimage for $\mathfrak{p}$.

For (2), pick a $J \subset B$ and let $I = A \cap J$. Thus, $A/I \hookrightarrow B/J$ is integral, so $\operatorname{Spec}(A/I) \twoheadleftarrow \operatorname{Spec}(B/J) = V(J) \subset \operatorname{Spec}(B)$. However, $\operatorname{Spec}(A/I)$ is just $V(I) \subset \operatorname{Spec}(A)$, so closed sets are sent to closed sets.

Notice that if $A \to B$ is non-injective, (1) can fail (look at $A/\ker(\varphi) \hookrightarrow B$), but (2) still holds.

For (3), choose $\mathfrak{p}_0 \subset \mathfrak{p}_1$ in A, and suppose $\mathfrak{q}_0$ is over $\mathfrak{p}_0$; then, take $A/\mathfrak{p}_0 \hookrightarrow B/\mathfrak{q}_0$. Using (1), there exists a preimage $\mathfrak{q}_1/\mathfrak{q}_0$ of $\mathfrak{p}_1/\mathfrak{p}_0$ (it must be a quotient of $\mathfrak{q}_0$ because, well, what are the prime ideals of $\mathfrak{p}_1/\mathfrak{p}_0$?). Then, $\mathfrak{q}_1$ satisfies the necessary conditions.

For (4), suppose $\mathfrak{q}$ and $\mathfrak{q}'$ are both over $\mathfrak{p}$, and $\mathfrak{q} \subseteq \mathfrak{q}'$. If we don't know what else to do, we might as well try localization. Now, $A_\mathfrak{p} \hookrightarrow B_\mathfrak{p}$, with $\mathfrak{p}A_\mathfrak{p}$ maximal and $\mathfrak{q}B_\mathfrak{p} \subseteq \mathfrak{q}'B_\mathfrak{p}$. By Lemma 20.2, $\mathfrak{q}B_\mathfrak{p}$ is maximal, so $\mathfrak{q}B_\mathfrak{p} = \mathfrak{q}'B_\mathfrak{p}$, and by the usual correspondence of maximal ideals in localization, $\mathfrak{q} = \mathfrak{q}'$. ⊠

The geometric content is that if k is algebraically closed and $k[x_1, \ldots, x_n] \hookrightarrow k[y_1, \ldots, y_m]$ is integral, then we can view them in affine space as $X \subset k^n$ and $Y \subset k^m$, and suppose $\pi : Y \to X$ is the induced map. Then, points (i.e. homomorphisms) go to points. If we have an irreducible $W \subset X$ with dimension d (where dimension will be formalized next week), then $\pi^{-1}(W)$ must also have an irreducible component of dimension d.

Dimension will be a generalization of transcedence degree, and related to chains of prime ideals (related to the notion that a surface in 3-space is two-dimensional, because it contains curves which contain points). Thus, dimension will be defined as the maximum length of a chain of prime ideals. But the Going-Up theorem says that chains get sent to chains, which is good.

The Going-Up theorem is an existence theorem for points (by the Nullstellensatz, a statement about prime ideals gets turned into one about points; the Nullstellensatz is also in some sense an existence theorem for points). It's actually rather easy to apply the abstract Going-Up theorem into a proof of the Nullstellensatz, by just interpreting it in the finitely generated case.

Theorem 20.3 (Going-Down). *Let A and B be integral domains, A be integrally closed (i.e. in its field of fractions) and $A \hookrightarrow B$ be integral. Then, if $\mathfrak{p}_0 \subseteq \mathfrak{p}_1$ are prime ideals of A and $\mathfrak{q}_1 \subset B$ is over $\mathfrak{p}_1$, then there exists a prime ideal $\mathfrak{q}_0 \subset \mathfrak{q}_1$ of B that is over $\mathfrak{p}_0$.*

We'll prove this theorem a little later.

Notice the stronger assumptions made here; otherwise, it's pretty symmetric to statement (3) of Theorem 20.1, and the other parts don't really make sense in this context.

On Friday, we're going to enhance A and $\operatorname{Spec}(A)$ with a "sheaf of functions." The analogue is in differential topology, where if M is a C^∞ smooth manifold, then for any open $U \subset M$, we have the set $\Gamma(U)$ of smooth functions $U \to \mathbf{R}$. Then, if $V \hookrightarrow U$, there's a natural map $\Gamma(U) \to \Gamma(V)$ given by restriction. Finally, the "sheaf axiom" allows functions to be glued together: if one is given $U = \bigcup_i U_i$ and $(f_i) \in \prod \Gamma(U_i)$, with $f_i|_{U_i \cap U_j} = f_j|_{U_i \cap U_j}$ for all i and j, then there's a unique $f \in \Gamma(U)$ such that $f|_{U_i} = f_i$.

We'll start with $\operatorname{Spec}(A)$; to each basic open X_a, assign the ring $A[1/a]$: we want to imitate the ideas from differential topology, but with functions coming from a. Then, there will be a version of the sheaf axiom. This can

[51] Here, $A_\mathfrak{p} = S^{-1}A$, where $S = A \setminus \mathfrak{p}$, and $B_\mathfrak{p}$ is defined the same way. Since $\mathfrak{p}$ is prime, S is multiplicative.

be souped up to arbitrary open sets of Spec(A), but the associated rings don't have nice names; one has to go back to the sheaf axioms, and it's a bit technical.

Another thing one can do with manifolds is this: for a manifold M and point $p \in M$, consider neighborhoods U of M directed by inclusion. Then, $\Gamma_p = \varinjlim_{p\in U} \Gamma(U)$ is the set of germs of smooth functions near p, in which $f \sim g$ if $f = g$ in any neighborhood of p. Γ_p is a local ring, whose maximal ideal is the functions vanishing at p (because if $f(p) \neq 0$, then $1/f$ is smooth in a neighborhood of p, so f is invertible in Γ_p). The analogy in Spec(A) is that if $\mathfrak{p} \in \mathrm{Spec}(A)$, we get the same limit: $\varinjlim_{\mathfrak{p}\in X_a} A[1/a] = A_{\mathfrak{p}}$.

21. Sheaves of Functions: 2/21/14

Today, we'll discuss some geometric intuition for the Going-Up theorem (Theorem 20.1) before moving on to schemes. Today's lecture was also by Greg Brumfiel.

Let $B = k[y_1,\dots,y_m]/J$ and $A = k[x_1,\dots,x_n]/I$ be affine varieties, where k is algebraically closed. Then, suppose $A \hookrightarrow B$ is integral. If $W = \underline{Z}(J)$ and $X = \underline{Z}(I)$, then $W \xrightarrow{\pi} X$.

A prime $\mathfrak{p} \subset A$ is an irreducible subvariety Y of X, as bigger ideals have fewer zeroes. Intuitively, its dimension is the transcedence degree of the field of fractions $A/\mathfrak{p}$ (though, again, we'll treat this more rigorously in the next lecture), and $\pi^{-1}(Y)$ has a d-dimensional irreducible component.[52]

The true content of Theorem 20.1 is that if $Y_{\mathfrak{p}} \supset Y$ (given by $\mathfrak{p}_1 \supset \mathfrak{p} \supset I$), then any such irreducible component $\pi^{-1}(Y)$ contains an irreducible piece of Y. The surjectivity of π^{-1} isn't always sufficient: surjectivity on primes for all rings and surjectivity for primes on one specific ring are different notions. Sometimes, though, the preimage isn't useful.

π^{-1}, as a set map, is also finite-to-one, which merely says that $B/\mathfrak{q}$ is finite algebraic over $A/\mathfrak{p}$. Generally, for the super-abstract modern algebraic geometry, it's helpful to think back to cases such as these and think about what you're actually saying; this finite-to-one property means there are only finitely many possible solutions given a bunch of coefficients. This relates to the correspondence of maximal ideals to maximal ideals in the affine algebraic case. Another way of thinking about it is that for integral extensions, there can't be infinite singularities in the corresponding varieties.

Sheaves. The goal for a sheaf is to carry over the notion of manifolds as an analogy: if M is a manifold and $U \subset M$ is open, then denote $\Gamma(U)$ to be the set of smooth functions $U \to \mathbf{R}$. Then, if $U = U_1 \cap \cdots \cap U_n$, then $f \mapsto f|_{U_i}$ gives maps

$$\Gamma(U) \longrightarrow \prod_i \Gamma(U_i) \rightrightarrows \prod_i \prod_j \Gamma(U_i \cap U_j).$$

Then, given $(f_i) \in \prod \Gamma(U_i)$, there exists an $f \in \Gamma(U)$ such that $f|_{U_i} = f_i$ iff the f_i agree when we pass to the intersection. We will want this analogy to hold with Spec(A) in place of M.

Part of the structure of a manifold M is its set $V_n \subseteq \mathbf{R}^n$ of basic opens (with some overlap), and these correspond to the basic opens of Spec(A). In manifolds, a key way to formulate these concepts is the notion of arbitrarily small open sets. When $X = \mathrm{Spec}(A)$, when does $X_a \supset X_b$? The answer is that $X_a \supset X_b$ is equivalent to any of the following:

- $V(a) \subseteq V(b)$.
- $b \in \sqrt{(a)}$.
- $b^n = ac$ for some $n \in \mathbf{N}$ and $c \in A$.
- a is invertible in $A_b = A[1/b]$ (since this implies $1/a = c/b^n$).
- Using the universal property of localization, the existence of maps making the following diagram commute.

$$\begin{tikzcd} A_a \arrow[rr] & & A_b \\ & A \arrow[ul] \arrow[ur] & \end{tikzcd}$$

This corresponds to a "restriction" $A_a \to A_b$, akin to restriction of functions in the manifold case.

Next, to each basic open associate a ring: $\Gamma(X_a) = A_a$. Thus, if $X_b \subseteq X_a$, then $A_a \to A_b$ holds by the above, and so $\Gamma(X_a) \to \Gamma(X_b)$, as in the case of manifolds.

If $\mathfrak{p} \in X$, where $\mathfrak{p} \subset A$, then $\varinjlim_{a\notin\mathfrak{p}} A_a \xrightarrow{\sim} A_{\mathfrak{p}}$ (where the limit is directed with respect to the above restrictions $A_a \to A_b$ whenever $X_a \supseteq X_b$, which is unique). Why is this? Well, every $f/g \in A_{\mathfrak{p}}$ is such that $g \notin \mathfrak{p}$, so it must

[52]Though this looks like going down, contravariance means it's actually going-up.

exist within some neighborhood. It's not hard to prove this is an isomorphism, though surjectivity ends up being a denominator chase.

There are other ways of proving this, such as checking that one satisfies the universal property of the other. A map out of $\varinjlim A_a$ is a bunch of ways of mapping out of the A_a, and so on. It's unclear if this works around the tricky part of directly[53] applying the definition. But the first proof offers some more intuition about what it means; why do they fit together? Why are they compatible? It takes some care.

So, awkwardly enough, we've never formally defined a sheaf. So it seems natural to not prove the statement we've been working towards: that Spec(A), as a union of basic opens, satisfies the sheaf axioms we've been vaguely talking about. Specifically, f_i/a_i^n and f_j/a_j^m agree in $A_{a_i a_j}$ iff there exists an $f \in A$ such that $f/1 \mapsto f_i/a_i^n$ for all i. This also corresponds to $X_a \cap X_{a'} = X_{aa'}$.

One has to be careful with this proof that we didn't get to see; it's fairly easy if A is an integral domain, because one can just work in the field of fractions, though. In some sense, the a_i generate the unit ideal $A = (a_i)$, so 1 is a linear combination of the a_i. One way to see a simpler proof of this is to just think about it when $X = X_a \cup X_b$.

For a general open $U \subset X = \operatorname{Spec}(A)$, $U = \bigcup X_{a_i}$, though this union isn't necessarily finite. It gets a little trickier, but one can use the sheaf axiom to say what $\Gamma(U)$ is; then, it's necessary to prove a "super-sheaf axiom" that's a bit too technical for this course. Alternatively, instead of using $\Gamma(X_{a_i})$, one can use "locally constant" functions with values $s(\mathfrak{p}) \in A_\mathfrak{p}$ for all $\mathfrak{p} \in U$. Then, $U \to \prod_{\mathfrak{p}\in U} A_\mathfrak{p}$, so if $s(\mathfrak{p}) = f/g$, then it can be restricted to lots of primes near $\mathfrak{p}$.

In integral domains, life is much easier: let A be a domain and K be its field of fractions. Then, it turns out that $\Gamma(U)$ is the set of $r \in K$ such that for all $\mathfrak{p} \in U$, $r = f_\mathfrak{p}/g_\mathfrak{p}$, where $g_\mathfrak{p} \notin \mathfrak{p}$. In other words, r is everywhere locally a rational function. This isn't true more generally, even in reduced rings.

Note that, while this was inspired by manifolds, plugging it back into the manifold case doesn't get us exactly back to where we began. It's an analogy, not a generalization.

A final interesting fact is that if k is algebraically closed and $U = \operatorname{Spec}(k[x,y] \setminus (0,0))$, then $U = A_x \cup A_y$ (where $A = k[x,y]$), because either $x \neq 0$ or $y \neq 0$, but $\Gamma(U) = k[x,y]$. Thus, there's nothing that's rational everywhere; things have to vanish on some curve.

22. Dimension Theory: 2/24/14

Brian Conrad is back today.

Dimension theory is a nice blend betwen the concepts of transcedence degree, geometry, and varieties. The goal is to be able to discuss this in the context of Noetherian rings, which is sort of a long saga, so we can start by considering finitely generated rings over an algebraically closed field. The more general dimension theory is a powerful way to handle problems, just like in linear algebra.

The basic idea is to start with a ring R, finitely generated over an algebraically closed field k. Thus, we have an extension $k[X_1, \dots, X_d] \hookrightarrow R$ for some d. If R is a domain, we also have $k(X_1, \dots, X_d) \hookrightarrow \operatorname{Frac}(R) = K$ as a finite extension over k. Thus, $d = \operatorname{trdeg}(K/k)$.[54] Geometrically, this means MaxSpec(R) is a covering of affine space $\mathbf{A}_k^d$.

We also want dimension to correspond to lengths of strictly increasing chains of prime ideals (equivalently, of irreducible closed sets), which is more intrinsic. To make this work, we'll need some basic properties of prime ideal chains within module-finite ring extensions $A \hookrightarrow B$. This allows one to lift chains of prime ideals from $k[X_1, \dots, X_d]$ into the more nebulous R. However, the preimage of something irreducible doesn't always remain so (e.g. if two lines map down onto one line).

The specific tool we need for this is the Going-Up theorem (Theorem 20.1): if $A \hookrightarrow B$ is integral and $\mathfrak{p}$ lifts to $\mathfrak{q}$, then a $\mathfrak{p}' \supset \mathfrak{p}$ lifts to a $\mathfrak{q}' \supset \mathfrak{q}$. Geometrically, let $V = \underline{Z}(\mathfrak{p})$ and $V' = \underline{Z}(\mathfrak{p}')$, and let $\pi : \widetilde{V} \twoheadrightarrow V$ be the counterpart to the integral map. Then, $k[V] \hookrightarrow k[\widetilde{V}]$ is module-finite; furthermore, the image is closed and dense, because $k[V] \hookrightarrow k[\widetilde{V}]$ hits 0, which is the generic point. Then, the fibers are really finite, because it's finite-dimensional as a k-algebra.

The idea is that the "highest-dimensional" irreducible component of $\pi^{-1}(V')$ should map to V'; it corresponds to some prine ideal. This is because $A/\mathfrak{p} \hookrightarrow B/\mathfrak{q}$ is an integral map of domains; without loss of generality, assume $\mathfrak{p}, \mathfrak{q} \neq (0)$, since we can take $\mathfrak{p}'/\mathfrak{p}$. Then, Spec($B$) $\to$ Spec(A) has closed image, but it's dense (since it hits (0), the generic point). Thus, it's surjective, so your prime lifts.

The Going-Down theorem (Theorem 20.3) is more geometrically subtle.

[53]No pun intended.

[54]The transcedence degree of an extension, written trdeg(K/k), was defined on the homework as the maximal number of algebraically independent functions on that extension, and similarly in the case of a variety.

23. More Dimension Theory: 2/26/14

24. Completions and the I-adic Topology: 2/28/14

25. Dedekind Domains: 3/3/14

26. Group and Galois Cohomology: 3/5/14

27. Applications of Group Cohomology: 3/7/14

28. Hilbert's Theorem 90: 3/10/14

29. Profinite Group Cohomology: 3/12/14

30. The Étale Topology: π/14