MATH 210B: Modern Algebra II

Lecturer: Professor Daniel Bump

Notes by: Andrew Lin

Winter 2023

Introduction

Professor Bump's office hours will be held before class from 12:15 to 1:15 (on Mondays, Wednesday, and Fridays), and Ben Church (the CA) will also hold office hours on Tuesdays and Thursdays. Information about the course can be found at http://sporadic.stanford.edu/Math210B/ (and also linked on Canvas).

This class covers two areas of mathematics that are pretty disjoint from each other (because they both appear on the qualifying exam), so we'll have five weeks of one topic and five weeks of another. We'll have some topics in commutative algebra (specifically, affine algebraic geometry) and also some in group representation theory. For more specifics on the first half, we'll start by discussing integral dependence and transcendence degree, leading into basic facts from algebraic geometry (primes in integral extensions, going-up and going-down), and then we'll talk about dimension theory and primary decomposition. A useful general reference (just like for 210A) is Lang's *Algebra*, and Atiyah and Macdonald's *Introduction to Commutative Algebra* will be useful for this first half of the course as well.

Our first homework assignment is already posted (due next week), and we should submit it on Gradescope.

1 January 8, 2023

For today, all rings will be commutative with a unit (denoted 1).

Definition 1

Let $A \subset B$ be two rings, and let $\alpha \in B$. We say that α is **integral** over A if $f(\alpha) = 0$ for some **monic** polynomial $f \in A[x]$ (that is, $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ for some $a_i \in A$).

This is similar to the definition for fields, but it is a bit more delicate.

Proposition 2

The following are equivalent:

1. α is integral over A,
2. The ring $A[\alpha]$ generated by A and α is finitely generated as an A-module,
3. There exists a faithful $A[\alpha]$-module which is finitely generated as an A-module.

Proof. For (1) implies (2), if we have some monic polynomial f with $f(\alpha) = 0$ as before, then $A[\alpha] = A \oplus A\alpha \oplus \cdots \oplus A\alpha^{n-1}$. And this is closed under multiplication, because α^n is a linear combination of lower powers $-a_{n-1}\alpha^{n-1} - \cdots - a_0$, and we can write similar relations for higher powers of α. So we are indeed finitely generated as an A-module.

For (2) implies (3), first recall that an R-module M is **faithful** if $rm = 0$ for all $m \in M$, then $r = 0$. So we can take $M = A[\alpha]$ (thought of as the direct sum above), and this is faithful because $\beta M = 0$ means that $\beta 1 = 0$ and thus $\beta = 0$.

Finally, for (3) implies (1), let M be a faithful $A[\alpha]$-module finitely generated as an A-module. We'll do this with linear algebra: suppose $x_1, \cdots, x_m$ generate M as an A-module, so αx_i is a linear combination of the x_is as well. Write $\alpha x_i = \sum_{j=1}^{m} a_{ij} x_j$ for $a_{ij} \in A$; then the matrix T with entries $a_{ii} - \alpha$ on the diagonal and a_{ij} off the diagonal maps $\begin{bmatrix} x_1 \\ \vdots \\ x_m \end{bmatrix}$ to the zero vector. We want to deduce that the determinant of T is then zero, because then the determinant will be a monic polynomial in α. Indeed, T has an adjugate matrix T^* such that $T^*T = \det(T)\mathrm{Id}$ (explicitly, the (i,j) entry is the determinant of the minor obtained by deleting the ith row and jth entry), and applying both sides to $\begin{bmatrix} x_1 \\ \vdots \\ x_m \end{bmatrix}$ yields zero on the left side. Thus $\det(T)$ annihilates all x_is, and **since the module is faithful** that means $\det(T) = 0$, giving us the desired polynomial proving integrality of α. □

Proposition 3

If $A \subset B$ are rings and $\alpha, \beta \in B$ are integral over A, then so are $\alpha + \beta$ and $\alpha\beta$. Thus, the elements of B that are integral over A form a ring.

Proof. Suppose $f(\alpha) = 0$ with $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ and $g(\beta) = 0$ with $g(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_0$. Then $A[\alpha, \beta]$ (the ring generated by A, α, and β) can be written as

$$A[\alpha, \beta] = \sum_{i \le n-1, j \le m-1} A\alpha^i \beta^j$$

(not necessarily a direct sum) because this is closed under multiplication by α and β (again by reducing higher powers with f and g). This is a faithful module because it contains the identity, and it is finitely generated as an A-module, so by criterion 3 of Proposition 2 the sum and product are both integral over A. (Here, note that we're thinking of $A[\alpha, \beta]$ as an $A[\alpha + \beta]$-module in one case and an $A[\alpha\beta]$ module in the other.) □

Definition 4

Let $A \subset B$ be rings. We say that B/A is **integral** (in other words, an integral extension of rings) if every element of B is integral over A.

Proposition 5

Let $A \subset B \subset C$ be rings. If B/A is integral and C/B is integral, then C/A is integral.

Proof. Suppose $\gamma \in C$. By integrality of C/B, there is some monic polynomial $f \in B[x]$ with $f(\gamma) = 0$, which we may write as $x^n + b_{n-1} + \cdots + b_0$. Note that it's not true that the ring B is finitely generated over A. However, we can say that

γ is integral over the ring $B_0 = A[b_0, \cdots, b_{n-1}]$, and B_0 is finitely generated as an A-module because the b_i are integral over A. (In particular, if b_i satisfy a monic polynomial of degree d_i, then $A[b_0, b_1, \cdots, b_{n-1}] = \sum_{k_i<d_i} Ab_0^{k_0} b_1^{k_1} \cdots b_{n-1}^{k_{n-1}}$ is closed under multiplication by any b_i, so it is a ring.) Now $M = B_0[\gamma]$ is finitely generated as a B_0-module and thus as an A-module (we can write it as the sum $\sum_{k_i<d_i, t<n} Ab_0^{k_0} b_1^{k_1} \cdots b_{n-1}^{k_{n-1}} \gamma^t$), so by criterion 3 of Proposition 2 γ is integral over A. □

Definition 6

Let $A \subset B$ be rings. We say that A is **integrally closed in B** if for any $\beta \in B$ integral over A, β is actually an element of A.

In other words, we can look at the ring of elements A' of B integral over A (which contains A), and if $A' = A$ then we are integrally closed. And this is consistent with the terminology in topology, where being "closed" is the same as being equal to the integral closure:

Definition 7

For any rings $A \subset B$, we call the set $\{\beta \in B : \beta \text{ integral over } A\}$ the **integral closure** of A in B.

To ensure this terminology is good, we must check the following fact:

Proposition 8

The integral closure of A in B is integrally closed in B.

Proof. Let A' be the integral closure of A in B, and let A'' be the integral closure of A' in B. Since A'/A is integral and A''/A' is integral, then A''/A is integral by Proposition 5. So by definition A'' is contained in A' and thus $A'' = A'$. □

Definition 9

Let A be an integral domain and F be its field of fractions. We say that A is **integrally closed** if A is integrally closed in F.

(In other words, if we omit the larger ring, then we are looking with respect to the field of fractions.)

2 January 11, 2023

Last time, we defined what it means for an element of a ring $\alpha \in B \supset A$ to be integral over A (for rings A, B commutative with unit), namely that α is the root of a monic polynomial in $A[x]$. We found that these integral elements form a ring, called the integral closure of A in B, and that for any integral elements $\alpha_1, \cdots, \alpha_n$, $A[\alpha_1, \cdots, \alpha_n]$ is a finitely generated A-**module** (not just a finitely generated A-algebra) because we can write it as a (not necessarily direct) sum $\sum A\alpha_1^{k_1} \cdots \alpha_n^{k_n}$ over all $k_i < d_i$ (where d_i is the degree of the polynomial f_i for integrality of α_i), which is closed under multiplication by applying f_is.

We then said that B/A is an integral extension of rings if all elements of B are integral over A and proved that if C/B and B/A are integral, then so is C/A. This makes it possible to define the integral closure of A in B (the set of integral elements over A) and show that "the closure of the closure is again the closure."

Today, we'll start by discussing how localization relates to these concepts. Recall that if A is a ring, a subset S is **multiplicatively closed** if it contains 1 and is closed under multiplication. We can then define the localization $S^{-1}A$ to be the set of symbols $\{\frac{a}{s} : a \in A, s \in S\}$ under the equivalence relation where $\frac{a}{s} = \frac{b}{t}$ if $u(at - bs) = 0$ for some $u \in S$ (if A is an integral domain it's enough just to check that $at - bs = 0$). This localization is the "smallest ring that contains A in which the elements of S become invertible," – in other words, there is a homomorphism $i : A \to S^{-1}A$ sending a to $\frac{a}{1}$ which is injective if A is an integral domain, and there is a universal property that any other such homomorphism from A to a ring in which element of S become units factors through A.

Proposition 10

Suppose B is integral over A, and $S \subset A$ is multiplicatively closed. Then $S^{-1}B$ is integral over $S^{-1}A$. (More precisely, there is a homomorphism $f : S^{-1}A \to S^{-1}B$ which maps $\frac{a}{s}$ to $\frac{a}{s}$, such that $S^{-1}B$ is integral over the image of f. This is just to avoid issues with f possibly having a kernel.)

Proof. Any element of $S^{-1}B$ can be written in the form $\frac{b}{s}$ for some $b \in B$ and $s \in S$. Since B is integral over A, we have $b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$ for some $a_i \in A$. But then we see that

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

which is a monic polynomial in $S^{-1}A[x]$ for which $\frac{b}{s}$ is a root. □

Proposition 11

If A is an integral domain which is integrally closed (in its field of fractions F), and $S \subset A$ is multiplicatively closed, then $S^{-1}A$ is also integrally closed.

Proof. In this case A is an integral domain, so we don't need to worry about the inclusion of $S^{-1}A$ in F. Notice that $S^{-1}A$ and A have the same field of fractions F – our goal is to show that if an arbitrary element $\frac{a}{b}$ of F is integral over $S^{-1}A$, then it is in $S^{-1}A$. The issue is basically that b is not assumed to be in S, but by integrality we get an equation of the form

$$\left(\frac{a}{b}\right)^n + \left(\frac{c_{n-1}}{s_{n-1}}\right)\left(\frac{a}{b}\right)^{n-1} + \cdots + \frac{c_0}{s_0} = 0,$$

where the s_is are in S. Multiplying everything by $(s_0 s_1 \cdots s_{n-1})^n$, we get a monic polynomial with coefficients in A for which $\frac{as_0 s_1 \cdots s_{n-1}}{b}$ is a root. But because A is integrally closed, this must be an element of A, and thus $\frac{a}{b} = \frac{1}{s_0 s_1 \cdots s_{n-1}} \cdot \frac{as_0 s_1 \cdots s_{n-1}}{b}$ is an element of $S^{-1}A$. □

Proposition 12

Any unique factorization domain A is integrally closed.

Proof. Suppose $\frac{a}{b} \in F$ is integral over A for some $a, b \in A$, such that a and b are coprime. Then we have a relation of the form

$$\left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + c_0 = 0.$$

Clearing denominators, we get an equation $c_{n-1}a^{n-1}b + \cdots + c_0 b^n = -a^n$. Thus any irreducible that divides b (meaning it divides every term on the left side) also divides a^n, meaning that it divides a because A is a UFD. Since we assumed a and b are coprime, this means b is indeed a unit. □

Example 13

For any field F, the polynomial ring $A = F[x]$ is a principal ideal domain, thus a UFD and thus integrally closed. Then $B = F[x, \frac{1}{x}]$ is a localization of A, specifically $S^{-1}A$ for $S = \{1, x, x^2, \cdots\}$, so it has the same field of fractions as A and thus cannot be integral over A (because no other elements of A's field of fractions are integral over it).

Example 14

Consider the ring B generated by two elements x, y given by the polynomial ring quotient $F[x, y]/(y^2 - x^2(x+1))$ (cautionary note: we may write $F[x, y]$ for the ring generated by F, x, and y, even though it's not a polynomial ring), and take $A = F[x]$. Then B is integral over A, because $y^2 - x^2(x+1) = 0$, and A and B are both integral domains. (Assume that the characteristic of F is not 2.)

However, we will show that B is not integrally closed (even though it is an integral extension of an integrally closed ring). Indeed, the field of fractions of A is $K = F(x)$, and the field of fractions of B is $E = F(x, y)$, the splitting field of the irreducible polynomial $y^2 - x^2(x+1)$. This is a quadratic extension of K, meaning that $[E : K] = 2$, and $t = \frac{y}{x} \in E$ is integral over A because $t^2 = \frac{y^2}{x^2} = x + 1$ but is not an element of K, thus also over B. But there is some polynomial in t not integral over B. To see that, notice that $C = F[t]$ contains B (since $t^2 = x + 1$ so $x \in C$, and then $y = tx$ so $y \in C$), and it has the same field of fractions as B. Assume without loss of generality that $C = B$. Then there is a homomorphism $\phi : C \to F$ sending $f(t)$ to $f(1)$ (the evaluation map) which sends t to 1 and thus $x = t^2 - 1$ to zero, meaning that y is also sent to zero. Thus $\ker(\phi)$ contains x and y, and (x, y) generates a maximal ideal in $B = C$ so $\ker(\phi) = Bx + By$ (because it can't be the whole ring). But this same argument works if we use a homomorphism $\psi : C \to F$ sending $f(t)$ to $f(-1)$, meaning $\ker(\psi) = Bx + By$ as well. This is a contradiction because $t + 1$ is in one kernel but not the other.

This example will become useful when we analyze prime ideals and transcendence degree next time.

3 January 13, 2023

Last time, we proved some properties related to integrality: specifically, we showed that $S^{-1}B$ is integral over $S^{-1}A$ if B is integral over A, and we also showed that $S^{-1}A$ is integrally closed (in the field of fractions F) if A is integrally closed. (A simpler way to phrase the proof from last time is that if $x \in F$ is integral over $S^{-1}A$, then we get an equation $x^n + \frac{c_{n-1}}{s_{n-1}}x^{n-1} + \cdots + \frac{c_0}{s_0} = 0$ with $s_i \in S$ for all i. But this yields a polynomial equation in $A[x]$ for which $s_0 \cdots s_{n-1}x$ is a root, so that element must be in A and thus $x \in S^{-1}A$.)

Today, we'll start our discussion of transcendence bases, transcendence degree, and Noether normalization. But first we'll prove one more result related to integrality:

Proposition 15

Let $A \subset B$ be rings with B integral over A, and let $\wp$ be a prime ideal. Then $\wp B$ is a proper ideal of B, and there is a prime ideal $\mathfrak{P}$ of B such that $\mathfrak{P} \cap A = \wp$.

Proof. We'll first prove the **special case** where A is a **local ring** and $\wp$ is its (unique) prime ideal. Suppose for the sake of contradiction that $\wp B$ is not proper. Then we can write $1 = b_1 p_1 + \cdots + b_n p_n$ for $b_i \in B$ and $p_i \in \wp$. Define $B_0 = A[b_1, \cdots, b_n]$; since the b_i are integral over A, B_0 is finitely generated as an A-module. Since $1 \in \wp B_0$, we also

have that $\wp B_0 = B_0$. But by Nakayama's lemma, since A is local with maximal ideal $\wp$ and M is a finitely generated A-module, $\wp M = M$ implies that $M = 0$. Since B_0 is nonzero, this gives a contradiction. Now for the **general case**, we can localize: let $S = A - \wp$ and consider the localizations $A_\wp = S^{-1}A$ and $B_\wp = S^{-1}B$ (here thinking of B as an A-module).

$$\begin{array}{ccc} A_\wp & \longrightarrow & B_\wp \\ \uparrow & & \uparrow \\ A & \longrightarrow & B \end{array}$$

From last lecture, we know that $B_\wp$ is integral over $A_\wp$, and we know that $(\wp A_\wp) \cdot B_\wp \neq B_\wp$. So if $\mathcal{P}'$ is a maximal ideal of $B_\wp$ that contains $\wp B_\wp$, then we must have $\mathfrak{P}' \cap A_\wp = \wp A_\wp$. (Note that because the homomorphism $A_\wp \to B_\wp$ is not necessarily injective, we're really saying that the preimage of $\mathfrak{P}'$ under that homomorphism is $\wp A_\wp$). So now taking the preimage of $\mathfrak{P}'$ in B (using the correspondence of ideals under localization) gives us the desired prime ideal $\mathfrak{P}$, which must indeed satisfy $\mathfrak{P} \cap A = \wp$. (We're basically completing the diagram above along the bottom right path.)

□

We'll state the condition from the previous proposition more explicitly:

Definition 16

If $A \subset B$ are rings and $\wp \subset A$ and $\mathfrak{P} \subset B$ are prime ideals, we say that $\mathfrak{P}$ **lies above** $\wp$ if $\wp = \mathfrak{P} \cap A$. A similar definition can be made if $\theta : A \to B$ is a homomorphism with $\wp = \theta^{-1}(\mathfrak{P})$.

This terminology is motivated by affine algebraic geometry, which is a topic we'll be discussing in this class:

Definition 17

Let F be a field. An **affine algebraic variety** over F is the set of solutions in F^n of some set of polynomial equations $\Sigma = \{f_1, \cdots, f_N\}$. Specifically, the variety $V(\Sigma)$ is the set $\{x \in F^n : f_i(x) = 0 \text{ for all } i\}$. This variety is also denoted $V(I)$, where I is the ideal generated by the elements $f_i \in F[X_1, \cdots, X_n]$. We say that $V = V(\Sigma)$ is **irreducible** if it is not the union of two proper subvarieties.

Example 18

The union of the x- and y-axis $V(X_1X_2)$ is not irreducible – in fact, irreducibility is equivalent to the **radical** $r(I)$ of the corresponding ideal $I = (X_1X_2)$ being prime. (The **radical** of an ideal I is the set $\{f \in R : f^n \in I \text{ for some } n\}$ – the binomial theorem proves that this is indeed an ideal.)

We can assume that I is equal to its radical, because $V(\Sigma) = V(I) = V(r(I))$ for some ideal I. (Indeed, if $f^n \in I$, then f^n vanishes on $V(I)$, which is the same as f vanishing on $V(I)$ because we're working in a field. In such a situation where we assume irreducibility (so $I = r(I)$ is prime), R/I will be an integral domain. (If we don't assume irreducibility we just get a reduced ring.) In fact, R/I is the space of all polynomial functions on V because two functions f, g are the same function on V if their difference is zero on all of I.

Example 19

We can now see an example where Proposition 15 doesn't hold if we don't have integrality of the extension. Consider the ideal $I = \langle XY - 1 \rangle \subset R = F[X, Y]$ – then the variety $V(I)$ is a hyperbola H, and it is irreducible.

The space of polynomial functions on this hyperbola H is then $B = R/I = F[x, y]$, where x and y are X and Y mod I, respectively, with $xy = 1$. In other words, B is basically $F\left[x, \frac{1}{x}\right]$, the **affine algebra** or **coordinate ring** $\mathcal{O}(H)$. If we then consider the polynomial map ϕ from H to the x-axis sending (X_1, X_2) to X_1, then we can compose a polynomial on the x-axis (thought of as just $F[x]$) with ϕ. Specifically, we get a ring homomorphism ϕ^* from $A = F[x]$ (functions on the x-axis) to $B = F[x, 1/x]$ (functions on H) sending f to $f \circ \phi$, which is the inclusion map.

But now the algebraic geometry idea is that **prime ideals roughly correspond to points** – if F is an algebraically closed field, there is a bijection between V (any affine variety) and **maximal** ideals of the ring of polynomial functions on V. (This is the **nullstellensatz**.) And the point is that the mapping is not surjective, since no point on the hyperbola projects to the origin, and thus there is no prime ideal of B lying above a prime ideal in A. And the reason the proposition from earlier doesn't apply is that $F[x, 1/x]$ is **not integral** over $F[x]$ (as we proved last time).

Example 20

On the other hand, if we take the example curve $y^2 = x^2(x+1)$ from last time and consider $A = F[x]$, $B = F[x, y]$, then we proved last time that B is integral over A. So if we believe the philosophy about prime ideals corresponding to points, then this corresponds to the fact that projecting the curve $y^2 = x^2(x + 1)$ on the x-axis is surjective (remembering that we are working over $\mathbb{C}$, not $\mathbb{R}$).

4 January 18, 2023

We'll briefly talk about transcendence degree today just to discuss the main facts, and then we'll move on to Noether normalization.

Definition 21

Let Ω be a field. A set of elements $\{y_1, \cdots, y_n\} \in \Omega$ is **algebraically independent** if there is no nonzero polynomial relation $\phi(y_1, \cdots, y_n) = 0$ between the y_is with coefficients in Ω (that is, $\Phi \in F[X_1, \cdots, X_n]$ is not the zero polynomial).

Definition 22

Suppose $F \subset K \subset \Omega$ are fields (we're going to put everything inside a big field Ω so that rings are all integral domains). A set of elements $x_1, \cdots, x_n \in K \subset \Omega$ **span** K over F if K is algebraic over $F(x_1, \cdots, x_m)$ (here parentheses means the **field** generated by F, $x_1, \cdots, x_m$, rather than just the algebra).

The word "span" here is technically incorrect (it's not like in the sense of linear algebra), but it's meant to provide some intuition similar to that of linear algebra. And this next result shows a further similarity (comparing the size of linear independent sets to spanning sets):

Theorem 23

Suppose $y_1, \cdots, y_n \in K$ are algebraically independent over F, and $x_1, \cdots, x_m \in K$ span K (meaning that $K/F(x_1, \cdots, x_m)$ is algebraic), then $n \leq m$.

In particular, this leads to the notion of a "trascendence basis" with well-defined size. And we can say something similar when our sets $\{x_i\}$ and $\{y_i\}$ are infinite, just using cardinality instead of size – however, this requires transfinite induction.

Proof. Since y_1 is algebraic over $F(x_1, \cdots, x_m)$ (by definition of the spanning set), there is a relation $\phi(y_1, x_1, x_2, \cdots, x_m) = 0$ for some nonzero polynomial ϕ in the polynomial ring over $m+1$ variables. This relation involves one of the x_is (because y_1 isn't algebraic over F by algebraic independence, so our polynomial can't just be in y_1). Without loss of generality say that ϕ involves x_1. Then this polynomial relation tells us that x_1 is algebraic over $F(y_1, x_2, \cdots, x_m)$ – in particular, K is algebraic over $F(x_1, y_1, x_2, \cdots, x_m)$, which is algebraic over $F(y_1, x_2, \cdots, x_m)$, and algebraic extensions stack. Thus $y_1, x_2, \cdots, x_m$ also span K.

We can then repeat this process: since y_2 is algebraic over $y_1, x_2, \cdots, x_m$, there is some nonzero $\psi \in F[Y_1, Y_2, X_2, \cdots, X_m]$ such that $\psi(y_1, y_2, x_2, \cdots, x_m) = 0$. Again ψ must involve one of the x_is because $\{y_1, y_2\}$ are algebraically independent. Letting it be x_2 without loss of generality, we see that K is algebraic over $F(y_1, y_2, x_2, \cdots, x_m)$, which is algebraic over $F(y_1, y_2, x_3, \cdots, x_m)$ (because x_2 is algebraic over the other variables). This means $\{y_1, y_2, x_3, \cdots, x_m\}$ also spans K. This same process shows that we can replace n of the x_is by y_is, so $n \leq m$ (if we had $n > m$ then we'd have $\{y_1, y_2, \cdots, y_m\}$ spanning K and then y_{m+1} is algebraic over $F(y_1, \cdots, y_m)$, contradicting linear independence). □

Remark 24. *There's a general notion of a* **matroid** *(where independence and span are concepts) which generalizes this kind of proof.*

Definition 25

Let $K \supset F$ be fields. A **transcendence basis** of K/F is a (possibly infinite) subset $\{y_1, y_2, \cdots\}$ such that the y_is are algebraically independent and span K (in the sense mentioned before that $K/F(y_1, y_2, \cdots)$ is algebraic).

Transcendence bases always exist by a Zorn's lemma argument – if we let Ω be the set of all algebraically independent subsets of K (over F), partially ordered by inclusion, then Ω is nonempty (because it contains $\{\varnothing\}$) and every chain has a maximal element (the union of the elements), there is some maximal element in the poset Ω. The point is that for any such maximal subset B, K must be algebraic over $F(B)$ because otherwise we could add a non-algebraic element to B. Thus B is a transcendence basis, and in fact by Theorem 23, any two transcendence bases have the same cardinality, and we will call that the **transcendence degree** and denote it $[K : F]_{\text{TD}}$. One important fact (which was an exercise for us) is that

$$[E : F]_{\text{TD}} = [E : K]_{\text{TD}} + [K : F]_{\text{TD}},$$

so transcendence degree is additive.

Theorem 26 (Noether normalization lemma)

Suppose $A = F[x_1, \cdots, x_n]$ is an integral domain with field of fractions $K = F(x_1, \cdots, x_n)$ (remember that these are not necessarily polynomial rings), and suppose the transcendence degree of K over F is r. Then there is some transcendence basis $\{y_1, \cdots, y_r\}$ such that $y_i \in A$ and A is integral over $F[y_1, \cdots, y_r]$. (Note that $F[y_1, \cdots, y_r]$ is actually a polynomial ring because the y_is are algebraically independent.)

There are two proofs of this in our textbook, but we'll do the first one which doesn't require us to treat the finite-field case separately.

Proof. Induct on the number of generators n. For the base case, if $x_1, \cdots, x_n$ are already algebraically independent over F, then $n = r$ is the transcendence degree and we can just take $x_i = y_i$ for all i. Otherwise, suppose there is an algebraic relation $\phi \in F[X_1, \cdots, X_n]$ such that $\phi(x_1, \cdots, x_n) = 0$. We will now introduce variables $z_1 = x_1, z_2 = x_2 - x_1^N, z_3 = x_3 - x_1^{2N}$, and so on (with N to be determined). Writing out the polynomial as $\phi = \sum_{j \in \mathbb{N}^n} a_j x^{(j)}$, where

$x^{(j)} = x_1^{j_1} x_2^{j_2} \cdots$ and $a_j \in F$, we can now rewrite this polynomial in terms of Zs. We know that

$$0 = \phi(x_1, \cdots, x_n) = \phi(z_1, z_2 + z_1^N, z_3 + z_1^{2N}, \cdots) = \sum_j a_j z_1^{j_1} (z_2 + z_1^N)^{j_2} (z_3 + z_1^{2N})^{j_3} \cdots,$$

and for sufficiently large N the degree of any particular summand j is $j_1 + Nj_2 + 2Nj_3 + \cdots$, coming from $a_j z_1^{j_1 + Nj_2 + 2Nj_3 + \cdots}$. Running through all of the summands, we can now cause a single term to dominate in degree. Specifically, we can say that $(j) > (j')$ if there is some k such that $j_k > j_{k'}$ and $j_{k+1} = j'_{k+1}, j_{k+2} = j'_{k+2}, \cdots$, and this is a total order (essentially lexicographic). Picking the j which is maximal under this ordering (across all j with nonzero coefficient a_j), we find that ϕ, as a polynomial in the z_is, has a leading term $a_j z_1^{j_1 + Nj_2 + \cdots}$. Since $a_j \in F$, this means $z_1 = x_1$ is integral over $F[z_2, \cdots, z_n]$, and remember that $F[z_1, z_2, \cdots, z_n]$ is the same ring as $F[x_1, \cdots, x_n]$. But by induction, there is a transcendence basis $\{y_1, \cdots, y_r\} \subset F[z_2, \cdots, z_n]$ (since we only have $(n-1)$ generators this time) such that $F[z_2, \cdots, z_n]$ is integral over $F[y_1, \cdots, y_r]$. (Importantly, the transcendence degree doesn't change because z_1 is algebraic over $F[z_2, \cdots, z_n]$.) Thus $A = F[x_1, \cdots, x_n] = F[z_1, z_2, \cdots, z_n]$ is integral over $F[z_2, \cdots, z_n]$, which is integral over $F[y_1, \cdots, y_r]$, and this is what we wanted to prove. □

5 January 20, 2023

Today's topic is **valuation rings**:

Definition 27

Let F be a field. A **valuation ring** is a subring R of F such that for any $x \in F$, either $x \in R$ or $x^{-1} \in R$.

Example 28

A **discrete valuation ring** is a principal ideal domain with a unique maximal ideal. For example, $\mathbb{Z}_{(p)}$ for a prime p is a discrete valuation ring in $\mathbb{Q}$, because any rational number as a reduced fraction has either numerator or denominator not divisible by p.

Example 29

$\mathcal{O}$, the ring of germs of holomorphic functions at $0 \in \mathbb{C}$ (that is, the set of power series $\sum_{i=0}^{\infty} a_i x^i$ with a positive radius of convergence) is a discrete valuation ring in the field of fractions $\{\sum_{i=-N}^{\infty} a_i x^i$ converging near zero$\}$).

Not all valuation rings are discrete valuation rings, but they are similar "in spirit," as we'll see in these next few results.

Proposition 30

Any valuation ring R is a local ring.

Proof. The set of non-units is easily seen to be closed under multiplication. For closure under addition, suppose $x, y \in \wp = R - R^\times$ are both non-units – we can just consider the case where x and y are nonzero. Then by definition either $\frac{x}{y}$ or $\frac{y}{x}$ is in R; without loss of generality say that $\frac{x}{y} \in R$. Then $1 + \frac{x}{y} = \frac{x+y}{y}$ is also in R. But then if $x + y$ is a unit, then multiplying by its inverse shows that $\frac{1}{y}$ is in R, contradicting that y is a unit.

In particular, the set of non-units yields a maximal ideal (adding any other element of R would give us the whole ring) and it must be the unique maximal ideal. Thus R is a local ring. □

Proposition 31

Any valuation ring R is integrally closed. In other words, if R is a valuation ring of its field of fractions F, then R is integrally closed in F.

Proof. Suppose $x \in F$ is integral over R. Then there is some polynomial relation $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, with $a_i \in R$. Suppose for the sake of contradiction that $x \notin R$. By definition of a valuation ring, we must have $x^{-1} \in R$, and in fact x^{-1} must be in $\wp$. But then we can rewrite the equation above as $1 = -\left(a_{n-1}x^{-1} + \cdots + a_0 x^{-n}\right)$, where the right-hand side is in $\wp$. Since $\wp$ is not the whole ring, this is a contradiction. □

Theorem 32 (Extension theorem for valuation rings)

Let F be a field and let $A \subseteq F$ be a ring. Suppose Ω is an algebraically closed field with $\phi : A \to \Omega$ a ring homomorphism. Then ϕ can be extended to a valuation ring of F containing A.

Proof. Let Σ be the set of pairs (R, Φ), where R is a ring $A \subset R \subset F$ and $\Phi : R \to \Omega$ is a ring homomorphism extending ϕ. By Zorn's lemma, Σ has some maximal element (which we'll denote (R, Φ)), meaning that we cannot extend $\Phi : R \to \Omega$ to a larger ring.

The first step is to prove that R is local. Because Ω is a field, the image of Φ in it must be an integral domain and thus $\ker(\Phi)$ is a prime ideal which we will call $\wp$ (this will be the $\wp$ we're looking for). Then Φ extends to $R_\wp$, via $\Phi\left(\frac{a}{s}\right) = \frac{\Phi(a)}{\Phi(s)}$ – this definition makes sense because s is not in $\wp$, so $\Phi(0)$ is nonzero and can be inverted in Ω, and it is well-defined because $\frac{a}{s} = \frac{b}{t}$ implies that $at = bs$, implying that $\Phi(a)\Phi(t) = \Phi(b)\Phi(s)$; multiplying by the inverses of $\Phi(t)$ and $\Phi(s)$ shows that $\frac{\Phi(a)}{\Phi(s)} = \frac{\Phi(b)}{\Phi(t)}$. But by maximality this means $R_\wp = R$ (since we can't extend beyond R), and this means R is a local ring (because it is the localization at a prime ideal).

Next, we want to show that R is indeed a valuation ring, meaning that for all nonzero $x \in F$ we want either $x \in R$ or $x^{-1} \in R$. The idea is to show that we can extend Φ to either $R[x]$ or $R[x^{-1}]$, since again by maximality that would mean $x \in R$ or $x^{-1} \in R$, respectively. Without loss of generality, we can assume that x is **algebraic** over R (otherwise $R[x]$ is a polynomial ring, so Φ can be extended to $R[x]$ by the universal property of the polynomial ring sending $\Phi(a_0 + a_1 x + \cdots + a_n x^n) = \Phi(a_0)$).

Lemma 33

We cannot have both $\wp R[x] = R[x]$ and $\wp R[x^{-1}] = R[x^{-1}]$.

Proof of lemma. Suppose that both of those equalities held. Then we could write

$$1 = a_0 + a_1 x + \cdots + a_n x^n = b_0 + b_1 x^{-1} + \cdots + b_n x^{-m}, \quad a_i, b_i \in \wp.$$

Choose such polynomials to minimize m and n; without loss of generality we may assume $n \geq m$. Notice that $1 - b_0$ must be a unit; otherwise it would be in the ideal of all non-units $\wp$ (here is where we use that R is local) and thus 1 would be in $\wp$. Thus we have

$$(1 - b_0)x^m = b_1 x^{m-1} + \cdots + b_m \implies x^m = b_1' x^{m-1} + \cdots + b_m'$$

where $b_i' = (1 - b_0)^{-1} b_i \in \wp$. But then multiplying this by $a_n x^{n-m}$ and subtracting it from the first relation allows us to reduce n by cancelling out the leading coefficient, which is a contradiction by minimality. □

So now without loss of generality we may assume that $\wp R[x]$ is a proper ideal of $R[x]$. Let $\mathfrak{P}$ be a maximal ideal of $R[x]$ containing $\wp R[x]$; then $\mathfrak{P} \cap R = \wp$ (because by construction the left-hand side contains $\wp$, it is an ideal of R, and $\wp$ is maximal in R). Then we have $R/\wp$ contained in $R[x]/\mathfrak{P}$ – these are both fields because the ideals are maximal in their respective rings, and in fact $R[x]/\mathfrak{P}$ is a finite extension of $R/\wp$ because x is assumed to be algebraic. From Φ we then get an induced injective homomorphism $\overline{\Phi} : R/\wp \to \Omega$ (since we define $\wp = \ker(\Phi)$). We can thus think of $R/\wp$ as being a subfield of the algebraically closed Ω, and thus we can extend to the finite extension and get a map $\overline{\Phi}' : R[x]/\wp \to \Omega$ (because the finite extension comes from adjoining algebraic elements, which will also lie in Ω). This then pulls back to a map $R[x] \to \Omega$, and that can only happen (by maximality) if $x \in R$. □

Fact 34

On a valuation ring $R \subset F$, we can introduce an **ordered group** $\Gamma = F^\times/R^\times$, where "ordered" means that there is a subset Γ^+ closed under multiplication (that is, a submonoid). Setting $\Gamma - = \{z : z^{-1} \in \Gamma^+\}$, we can then have $\Gamma^+ \cap \Gamma^- = \{1\}$, and we can think of this as the "positive reals" and the "negative reals." The ordering is then that $x < y$ if $y^{-1}x \in \Gamma^+$; in a discrete valuation ring Γ will be isomorphic to $\mathbb{Z}$. We then have $R/R^\times = \Gamma^+$, and a **valuation** is then a mapping sending $F^\times$ to this group – specifically, we have $\nu : F \mapsto \Gamma \cup \{-\infty\}$ so that 0 can have valuation $-\infty$. But we'll probably talk more about this later.

We'll see how this relates to the nullstellensatz next time.

6 January 23, 2023

We'll discuss the nullstellensatz today – this works best over an algebraically closed field, and that's what we'll do. There are actually two versions that we'll go over – recall that the **variety** of an ideal $\mathfrak{a}$, denoted $V(\mathfrak{a})$, is the locus of zeros of $\mathfrak{a}$.

Theorem 35 (Weak nullstellensatz)

Let F be an algebraically closed field, and let $R = F[x_1, \cdots, x_n]$ be a polynomial ring. If $\mathfrak{a} \subset R$ is a proper ideal, then $V(\mathfrak{a})$ (the set of $(a_1, \cdots, a_n) \in F^n$ with $f(a_1, \cdots, a_n) = 0$ for all $f \in \mathfrak{a}$) is nonempty.

In other words, every proper ideal has a zero. For the other statement, recall that for any set $X \subset F^n$ (usually a variety or algebraic set), we can define

$$I(X) = \{f \in F[X_1, \cdots, X_n] : f = 0 \text{ on } X\}.$$

By definition, we know that $I(V(\mathfrak{a})) \supset \mathfrak{a}$, but we could have $\mathfrak{a}$ a strict subset of $I(V(\mathfrak{a}))$. On the other hand, we can define the **radical**

$$r(\mathfrak{a}) = \{f \in R : f^n \in \mathfrak{a} \text{ for some } n\}.$$

To see that the radical is closed under addition, notice that that by the binomial theorem, we know that $(f+g)^N = \sum \binom{N}{i} f^i g^{n-i}$, and then if f, g are in the radical then for sufficiently large N $f^i g^{n-i}$ is always zero, so the sum is also zero.

Theorem 36 (Strong nullstellensatz)

Again let $\mathfrak{a} \subset F[x_1, \cdots, x_n]$ be any ideal. Then $I(V(\mathfrak{a})) = r(\mathfrak{a})$.

These results also apply to quotients of polynomial rings, so the nullstellensatz also applies to any finitely generated ring over an algebraically closed field – this is the fundamental connection of commutative algebra with affine algebraic geometry.

With our definitions, it is easy to see that $r(\mathfrak{a}) \subset I(V(\mathfrak{a}))$. Indeed, if $f \in r(\mathfrak{a})$, then $f^n \in \mathfrak{a}$ and thus $f^n = 0$ on $V(\mathfrak{a})$. Then f vanishes wherever f^n vanishes so $f \in I(V(\mathfrak{a}))$. But the other inclusion is harder.

Proof of equivalence of weak and strong nullstellensatz. To show that the strong nullstellensatz implies the weak nullstellensatz, first notice that we can assume without loss of generality that $\mathfrak{a}$ is maximal, since enlarging the set of polynomials only makes the set smaller. Then by maximality, $r(\mathfrak{a}) = \mathfrak{a}$. But if $V(\mathfrak{a})$ were empty, then we would have $I(V(\mathfrak{a})) = R$, which is a contradiction with the strong nullstellensatz because the two sides are not equal.

It turns out there is an implication the other way as well, which uses the "Rabinowitsch trick" (the proof was published by Rainich, who used a pseudonym to publish it). Suppose the weak nullstellensatz is true, and let f be some polynomial in $I(V(\mathfrak{a}))$. Introduce another indeterminate Y, so that (we'll use capital letters since we have a polynomial ring)

$$R = F[X_1, \cdots, X_n] \subset F[Y, X_1, \cdots, X_n].$$

Now consider the ideal $\mathcal{A}$ in R generated by $\mathfrak{a}$ and the polynomial $1 - Yf(X_1, \cdots, X_n)$. We claim this ideal has no zeros in F^{n+1} – that is, we claim that $V(\mathcal{A})$ is empty. Indeed, if $(b, a_1, \cdots, a_n)$ were a zero, then either **(1)** $(a_1, \cdots, a_n)$ is in $V(\mathfrak{a})$ (which would mean $f(a_1, \cdots, a_n) = 0$), meaning that $1 - Yf(X_1, \cdots, X_n)$ would have value 1 at $(b, a_1, \cdots, a_n)$ and thus not everything in $\mathcal{A}$ vanishes at this point, or **(2)** $(a_1, \cdots, a_n)$ is not in $V(\mathfrak{a})$, meaning there is some $\phi \in \mathfrak{a}$ with $\phi(a_1, \cdots, a_n) \neq 0$, meaning again that $(b, a_1, \cdots, a_n)$ cannot lie in $V(\mathcal{A})$. So $V(\mathcal{A})$ is empty, and that means that by the weak nullstellensatz, $\mathcal{A}$ must be the entire ring $R[Y] = F[X_1, \cdots, X_n, Y]$.

In particular, this means that $1 \in \mathcal{A}$, so we can write $1 = \sum b_i a_i + b_0(1 - Yf(X_1, \cdots, X_n))$, where $b_i \in R[Y]$ and $a_i \in \mathfrak{a}$. Working in the field of fractions – that is, the ring of rational functions in these variables – we can substitute $Y = \frac{1}{f(X_1, \cdots, X_n)}$ and find that

$$1 = \sum b_i \left(\frac{1}{f(X_1, \cdots, X_n)}, X_1, \cdots, X_n \right) a_i (X_1, \cdots, X_n),$$

still with $a_i \in \mathcal{A}$ and $b_i \in R[Y]$. But then if we multiply by a sufficiently large power of f to clear denominators in the b_i terms, we find that f^N is equal to a sum of terms which are each some polynomial times some element of $\mathfrak{a}$. Thus $f^N \in \mathfrak{a}$ and thus f (which we originally assumed was in $I(V(\mathfrak{a}))$ is also in $r(\mathfrak{a})$. □

So the two statements are equivalent, and it remains for us to prove the weak nullstellensatz. We'll first prove the "algebraic nullstellensatz," also called Zariski's lemma:

Proposition 37 (Algebraic nullstellensatz)
Let F be a field, and let K be a field containing F that is finitely generated as an F-algebra (that is, $K = F[x_1, \cdots, x_n]$ not as a polynomial ring but as an F-algebra). Then K is a finite (in particular algebraic) extension of F.

Proof. Here is where we use the extension theorem for valuation rings, as well as Noether normalization – the latter can be avoided with an alternative proof, though. By Noether normalization, there is a transcendence basis $y_1, \cdots, y_r$ of K over F such that $F[x_1, \cdots, x_n]$ is integral over $F[y_1, \cdots, y_r]$ (the latter of which is isomorphic to a polynomial ring in r variables). We can thus define the homomorphism $\phi : F[y_1, \cdots, y_n] \to \overline{F}$ which plugs in 0 for each y_i. This homomorphism then extends to a valuation ring R of K; furthermore, $R \supset F[y_1, \cdots, y_r]$ and R is integrally closed because it is a valuation ring. Thus R contains the integral closure of $F[y_1, \cdots, y_r]$, which is K. Thus using this

homomorphism we can map K to $\overline{F}$; this is a map between fields so it is an embedding. In particular, this means K is algebraic over F, and it's also finitely algebraically generated by definition, so it is a finite extension. (And this means $r = 0$.) □

To get from here to the weak nullstellensatz is easy: if $\mathfrak{m}$ is any maximal ideal of $F[X_1, \cdots, X_n]$, then $F[X_1, \cdots, X_n]/\mathfrak{m}$ satisfies the conditions of the algebraic nullstellensatz, so it is a finite extension of F. We'll talk more in detail about this next time!

7 January 25, 2023

We'll continue our discussion of algebraic geometry concepts today – the idea is that affine algebraic geometry and commutative algebra are almost the same, in that they talk about the same concepts. (There's three sets of lecture notes about the Zariski topology, varieties, and the going-up and going-down lemmas – the last of these will be covered soon in class.) This next definition should look familiar from our homework:

Definition 38

Let F be a field, which we assume to be algebraically closed (so that the nullstellensatz holds). An **affine algebraic set** $X \subset \mathbb{A}^n$ (where $\mathbb{A}^n$ is the **affine *n*-space** $\mathbb{F}^n$ as a set) is the set of all solutions of some set Σ of polynomial equations. We will write this as $X = V(\Sigma) = \{x \in \mathbb{A}^n : f(x) = 0 \text{ for all } f \in \Sigma\}$.

If we let $\mathfrak{a}$ be the ideal generated by Σ, then clearly $V(\Sigma) = V(\mathfrak{a})$, and in fact this is even equal to $V(r(\mathfrak{a}))$ (as we've discussed previously), where the radical of $\mathfrak{a}$ is the set $r(\mathfrak{a}) = \{f \in F[x_1, \cdots, x_n] : f^N \in \mathfrak{a} \text{ for some } N\}$. So we may assume Σ is an ideal, even a **radical ideal** (meaning that Σ is its own radical), since the radical of $r(\mathfrak{a})$ is again $r(\mathfrak{a})$. And as we showed, the set of subsets of $\mathbb{A}^n$ of the form $V(\mathfrak{a})$ for some $\mathfrak{a}$ forms a set of closed sets of a topology (it is closed under finite unions and arbitrary intersections), which we call the **Zariski topology**. Indeed, we have $V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{ab})$ (since the product of two ideals is generated by products of polynomials in $\mathfrak{a}$ and $\mathfrak{b}$), and $V\left(\sum_i \mathfrak{a}_i\right) = \bigcap_i V(\mathfrak{a}_i)$.

This topology on $\mathbb{A}^n$ is a bit strange in that it's not Hausdorff – in fact, any two nonempty open sets have nonempty intersection (so we can't separate any open sets at all). So some of our intuition with ordinary topological spaces may break down, but not all of it. The idea is that closed subsets of $\mathbb{A}^n$ correspond to radical ideals (with correspondence **order-reversing**), and the nullstellensatz says that two radical ideals with the same closed set are actually the same ideal. Furthermore, because $R = F[x_1, \cdots, x_n]$ is noetherian, that carries over to $\mathbb{A}^n$ as well via the correspondence – any **descending** chain of closed sets $X_1 \supsetneq X_2 \supsetneq \cdots$ must terminate. Such a topological space is then called noetherian as well:

Definition 39

A topological space is **noetherian** if any descending chain of closed subsets terminates, and it is called **irreducible** if it is not the union of two proper closed subsets.

In particular, $\mathbb{A}^n$ is both noetherian and irreducible. On the other hand, the union of the coordinate axes $X = \{(x, 0) : x \in \mathbb{A}\} \cup \{0, y : y \in \mathbb{A}\}$ in $\mathbb{A}^2$ is not irreducible – it's a closed set, but it's the union of its two parts, each of which is closed.

Proposition 40

Any noetherian space is the finite union of irreducible closed subspaces.

Proof. Let $x \in X$ be some arbitrary element, and let Y be a minimal closed subset of X containing x. (This exists by the nooetherian property and a Zorn's lemma argument on the closed subsets containing x, or alternatively we can just take the intersection of all closed subsets containing x.) Then Y must be irreducible, since we would otherwise be able to write $Y = Y_1 \cup Y_2$, and then either x is in Y_1 or Y_2; whichever it is, we contradict minimality of Y. So x is in some irreducible closed subset; we can take the union of the corresponding subsets over all x.

But we can in fact say that this union can be taken to be **finite** – this now actually uses the Noetherian property. Indeed, if we had an infinite union and none of them could be thrown away, we could find an infinite descending chain. (We'll talk more about this next time.) □

This decomposition is unique, since there is a unique smallest set of closed irreducible subsets (which we call the **components** of X). This means that for any closed set $X = V(\mathfrak{a}) \subset \mathbb{A}^n$ (where we take $\mathfrak{a} = r(\mathfrak{a})$), we can consider the topology on X induced by the Zariski topology on $\mathbb{A}^n$ (which we **also** call the Zariski topology). To see whether X is irreducible, notice that the ring of polynomials on X is $R/\mathfrak{a}$ (here is where we've used the nullstellensatz – f_1, f_2 have the same restriction to X if and only if $f_1 - f_2 = 0$ on X, which occurs if and only if $f_1 - f_2 \in r(\mathfrak{a}) = \mathfrak{a}$.)

We will call $\mathcal{O}(X) = R/\mathfrak{a}$ the **affine algebra** or **coordinate ring**. Notice that X is irreducible if and only if $\mathcal{O}(X)$ is an integral domain – if we have $f_1, f_2 \in \mathcal{O}(X)$ with $f_1 f_2 = 0$, then $X_i = \{x : f_i(x) = 0\}$ for $i \in \{1, 2\}$ are closed sets with $X = X_1 \cup X_2$, so irreducibility breaks unless either f_1 or f_2 is zero. So in fact irreducibility corresponds to **primeness** of the ideal $\mathfrak{a}$, and we will call irreducible affine algebraic sets **affine varieties**.

However, we have to dispense of the embedding into affine space if we want to understand the connection with commutative algebra more clearly – it shouldn't depend on the ambient space. The idea is that affine algebraic sets form a **category**, with morphisms given by polynomial maps: if we have $X \subseteq A^n$ and $Y \subseteq A^m$, then a map $f : X \to Y$ is a morphism if there exist polynomials $f_1, \cdots, f_n \in F[X_1, \cdots, X_n]$ with $f(x_1, \cdots, x_n) = (f_1(x_1, \cdots, x_m), \cdots, f_n(x_1, \cdots, x_m))$. Such a morphism then induces a ring homomorphism $f^* : \mathcal{O}(Y) \to \mathcal{O}(X)$ given by post-composition with f, and conversely any ring (F-algebra) homomorphism $\mathcal{O}(Y) \to \mathcal{O}(X)$ gives rise to a morphism. To see that, suppose $Y = F[X_1, \cdots, X_m]/\mathfrak{b}$ for some radical ideal $\mathfrak{b}$. Take generators $y_1, \cdots, y_m$ which are cosets modulo b and look at their images under the homomorphism, and then we can interpret $\phi(y_i)$ as some polynomial $f_i(x_1, \cdots, x_n)$ (or specifically the corresponding cosets). The point is that if these affine algebraic sets form a category, then isomorphic objects may correspond to different affine embeddings, which we do want to identify together.

Definition 41

A morphism $f : X \to Y$ between varieties is **dominant** if $f(X)$ is dense in Y (though not necessarily surjective).

Proposition 42

A morphism f is dominant if and only if the corresponding map $\mathcal{O}(Y) \to \mathcal{O}(X)$ is injective. In particular, for any dominant morphism we can identify $\mathcal{O}(Y)$ as a subring of $\mathcal{O}(X)$; if $\mathcal{O}(X)$ is integral over $\mathcal{O}(Y)$, then f is surjective.

(This fact is proved in next lecture.)

Example 43

Consider $X = V(X_1X_2 - 1)$, which is the hyperbola in $\mathbb{A}^2$, and $Y = \mathbb{A}^1$ the x-axis. Then $\mathcal{O}(X)$ can be thought of as $F[X_1, X_2]/(X_1X_2 - 1) = F[X, \frac{1}{X}]$ Then the map $f : X \to Y$ which is the projection onto the x-axis is dominant (because $F[X]$ injects into $F[X, \frac{1}{X}]$, and it has $\mathcal{O}(X)$ not integral over $\mathcal{O}(Y)$. And indeed f is not surjective (this is a similar example as we've seen in a previous class).

This whole argument can also be formulated in terms of prime ideals, which would motivate the next topic of "going-up" and "going-down." But we'll see that in the future!

8 January 27, 2023

Last time, we started discussing affine varieties and some relevant properties of their constructions. In the notes on the class website, some additional information about the irreducible decomposition of a noetherian topological space is posted – recall that a topological space is **noetherian** if every descending sequence $X_1 \supset X_2 \supset \cdots$ eventually terminates. Specifically, we saw that $\mathbb{A}^n(F)$ is noetherian, and more generally any algebraic set (affine variety) X is also closed. (Indeed, $\mathcal{O}(X) = R/\mathfrak{a}$ is noetherian by the Hilbert basis theorem, so the ascending chain condition for ideals yields the corresponding descending chain condition on closed sets.) The important takeaway is that if $X = V(\mathfrak{a})$ for some radical ideal $\mathfrak{a}$, then X is irreducible if and only if $\mathfrak{a}$ is prime.

Since we're going to turn to dimension theory soon, we'll go back to the proof that any noetherian space is the finite union of irreducible closed subspaces, slightly restating the statement:

Proposition 44

If X is a noetherian topological space, then we may write $X = X_1 \cup \cdots \cup X_n$ with X_i irreducible closed subsets. Furthermore, this decomposition is unique if we discard redundant factors, meaning that $X_i \subsetneq X_j$ for any i, j.

Proof. From our discussion last lecture, a Zorn's lemma argument tells us that (using lower bounds instead of upper bounds, and using the descending chain condition) a nonempty set of closed subsets always has a minimal element. Thus, if X does not have such a finite decomposition, let Σ be the set of all closed subsets $Z \subseteq X$ with Z not having a finite irreducible decomposition. By assumption Σ is nonempty because it contains X, so it has a minimal element Z. Z is also noetherian (since it's a closed subset of X), and Z is not irreducible (or else it would work as its own decomposition into irreducible factors). Thus we have $Z = Z_1 \cup Z_2$, and by minimality Z_1 and Z_2 do have finite irreducible decompositions. But putting those together, that means Z does have a finite decomposition, a contradiction.

The uniqueness is written up in notes and is relatively routine (just comparing components in two different representations). □

We're now ready to turn to **dimension**, for which there are two different definitions that will turn out to be equivalent. But to prove their equivalence, we'll need some of the results from earlier in this class, as well as the going-up and going-down lemma.

Definition 45

Let X be an affine variety (recall that for us this means it is an irreducible affine algebraic set). Then $\mathcal{O}(X)$ is an integral domain, meaning that it has some field of fractions K. The **dimension** of X is then the transcendence degree of K/F.

The idea is that for a dimension n variety, there should be n algebraically independent functions. And the way to interpret this dimension is to say that $\mathcal{O}(X)$ is rational over $F[y_1, \cdots, y_d]$, so we sort of have "rational functoins in d dimensions."

Definition 46

Again let X be an affine variety. The **combinatorial dimension** is the maximal d such that we have a chain $X_0 \subsetneq X_1 \subsetneq X_2 \subsetneq \cdots X_d = X$ of nonempty closed irreducible subspaces.

The idea is that the smallest possible chain starts with a point (which is 0-dimensional), then something like a line (which is 1-dimensional), and so on up until the entire variety X. The point is that if X and Y are irreducible subsets with $X \subsetneq Y$, then we want $\dim(Y) > \dim(X)$ (we don't want a situation where X is just the x-axis and Y is the union of the x- and y-axes). And we can make a corresponding definition on the commutative algebra side:

Definition 47

Let R be a ring. The **Krull dimension** of R, denoted $\dim(R)$, is the maximal d such that there is a chain of prime ideals $\wp_0 \subsetneq \wp_1 \subsetneq \cdots \subsetneq \wp_d$. (If R is an integral domain, then $\wp_0$ can be taken to be the zero ideal.)

Specifically, notice that the Krull dimension of $\mathcal{O}(X)$ is the combinatorial dimension of X, and the deeper result is that this is also the dimension of X in the transcendence degree definition. And remember that $\wp_d$ corresponds to X_0, $\wp_{d-1}$ corresponds to X_1, and so on.

Recall from last time that a morphism $f : X \to Y$ of varieties is **dominant** if $f(X)$ is dense in Y, and we stated that f is dominant if and only if the corresponding F-algebra homomorphism $f^* : \mathcal{O}(Y) \to \mathcal{O}(X)$ (given by precomposition with f) is injective. We'll now do the proof of this:

Proof. For any nonzero $\phi \in \mathcal{O}(Y)$, consider the set

$$Y_\phi = \{y \in Y : \phi(y) \neq 0\}.$$

This is the complement of the closed set $V((\phi))$, so it is open. In fact, Y_ϕ form a basis of the topology, since the complement of $V(\mathfrak{a})$ (for any $\mathfrak{a}$) is the union of Y_ϕs for any $\phi \in \mathfrak{a}$. (Indeed, if $x \notin V(\mathfrak{a})$, then $\phi(x) \neq 0$ for some $\phi \in \mathfrak{a}$, which is the same as saying that $x \in Y_\phi$ and thus $x \in \bigcup_{\phi \in \mathfrak{a}} Y_\phi$.) These Y_ϕs are sometimes called the **principal open sets**.

So now if f^* is not injective, then this is equivalent to $f^*(\phi) = 0$ for some nonzero $\phi \in \mathcal{O}(Y)$, which happens if and only if $f(X) \cap Y_\phi = \varnothing$ (in other words, $f^*(\phi) = \phi \circ f$ is the zero map). But that's the same as saying that $f(X)$ is not dense (since density requires intersecting every basic open set). □

We've already proved an **easy version of the going-up theorem** in this class (though a more complicated version can be seen in the lecture notes, which we should read). The result was as follows: let B be integral over A, and let $\wp$ be a prime ideal of A. Then $\wp B \neq B$, and B contains a prime ideal above A. (Recall that we proved $\wp B \neq B$ by a Nakayama lemma argument when B is a finite A-module, and even when it isn't we can still make the argument

work.) Now as an application, recall that we stated last time that if $f : X \to Y$ is a dominant morphism, then the map $\mathcal{O}(Y) \hookrightarrow \mathcal{O}(X)$ is injective, and if $\mathcal{O}(X)$ is integral over $\mathcal{O}(Y)$ then f is surjective. We'll prove that as well:

Proof. Let $y \in Y$ and consider $\mathfrak{m}_y = \{\phi \in \mathcal{O}(Y) : \phi(y) = 0\}$. This is a maximal ideal, and thus there is some ideal $\mathfrak{P}$ of $\mathcal{O}(X)$ lying above $\mathfrak{m}_y$ which turns out to be maximal. So by the nullstellensatz there is some $x \in X$ with $\{x\} = V(\mathfrak{P})$ (the key point is that **points are in bijection with maximal ideals**), and we can check that $f(x) = y$. □

9 January 30, 2023

We'll continue our discussion of dimension with the going-up and going-down theorems today. Recall that a (commutative) ring A's **Krull dimension** is defined by looking at the maximal length of a chain of prime ideals $\wp_0 \subseteq \cdots \subseteq \wp_d$, and that if A is an algebra over some ground field the transcendence degree of the field of fractions of A agrees with this. (Note that there are rings that are even finitely generated but still have infinite Krull dimension. But the rings in algebraic geometry and algebraic number theory are typically finite dimension.)

Definition 48

A **Dedekind domain** is an integrally closed Noetherian domain of dimension 1.

In other words, every nonzero prime ideal is maximal (since the longest possible chain would be $(0) \subseteq \wp$, here using that (0) is a prime ideal because we have a domain). A principal ideal domain is always a Dedekind domain, since any nonzero prime ideal is (f) for some irreducible element $f \in A$, and these are already maximal. But in general there are lots of rings that are Dedekind domains but not PIDs that we still care about.

Theorem 49

Let L/K be a finite separable extension, and suppose $A \subseteq K$ is a Dedekind domain. Then the integral closure B of A in L is also a Dedekind domain.

This is left to us as an exercise, and we should note that this result **does not** hold for principal ideal domains:

Example 50

If $L = \mathbb{Q}(\sqrt{-5})$ and $K = \mathbb{Q}$, and we take $A = \mathbb{Z}$ (which is a PID), then the integral closure of A in L is $\mathbb{Z}[\sqrt{-5}]$. This is not a principal ideal domain because unique factorization fails ($6 = 2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$), meaning it's not a UFD, but on the other hand it is a Dedekind domain.

The point is that Dedekind domains are a bit pathological, but localizing them gets us a discrete valuation ring and thus we're back in the world of PIDs.

Example 51

Suppose X is an affine algebraic curve (that is, an affine variety of dimension 1), then $\mathcal{O}(X)$ is a Dedekind domain if and only if X is **nonsingular** (we will define this later).

For illustration, $\mathbb{C}[X, Y | Y^2 = X^2(X+1)]$ is not integrally closed, so it is not a Dedekind domain. (The corresponding curve has a singularity at 0, and indeed $t = \frac{y}{x}$, which captures the "different slopes" near 0 for the curve, is in the

integral closure.) so it is not a Dedekind domain, but $\mathbb{C}[X, Y | Y^2 = X(X^2 - 1)]$ is an elliptic curve which is nonsingular, so the corresponding ring is a Dedekind domain.

We're now ready to talk about the going-up and going-down theorems, which tell us how chains of primes behave with respect to integral extensions. The original results come from a paper of Cohen and Seidenberg which can be found here.

Theorem 52 (Going up)
Let B/A be an integral extension of commutative rings. (Sometimes we require that A and B are integral domains.) Recall that a prime ideal $\mathfrak{P}$ of B is "above" a prime ideal $\wp$ of A if $\mathfrak{P} \cap A = \wp$. Then if $\wp_1 \subset \wp_2$ are prime ideals of A, and $\mathfrak{P}_1$ is a prime ideal of B above $\wp_1$, then there is a prime ideal $\mathfrak{P}_2$ of B above $\wp_2$ with $\mathfrak{P}_1 \subset \mathfrak{P}_2$. In fact, if $\wp_1 \subsetneq \wp_2$ then we may choose $\mathfrak{P}_2$ to be strictly larger than $\mathfrak{P}_1$.

Visually, we can imagine that we are trying to fill in the blue part of this diagram:

$$\begin{array}{ccc} \mathfrak{P}_1 & \subset & \mathfrak{P}_2 \\ \uparrow & & \uparrow \\ \wp_1 & \subset & \wp_2 \end{array}$$

Proof. We've proven previously that for any prime ideal $\wp$ of A, there is **some** prime of B that lies above it. We will let $\overline{A} = A/\wp_1$ and $\overline{B} = B/\mathfrak{P}_1$ – we then get a natural inclusion $\overline{A} \hookrightarrow \overline{B}$ (this is injective because anything in the kernel of the map $A \to \overline{B}$ would be in $\mathfrak{P}_1 \cap A = \wp_1$). Then $\overline{B}$ is still integral over $\overline{A}$, so we can apply that previous result to the prime ideal $\overline{\wp_2}$ of $\overline{A}$. Furthermore, in the previous proof it is clear that $\wp \neq 0$ implies $\mathfrak{P} \neq 0$, so we now get an ideal $\overline{\mathfrak{P}_2}$ of $\overline{B}$ above $\overline{\wp}_2$, and pulling that back to B yields an ideal $\mathfrak{P}_2$ above $\wp_2$ that contains $\wp_1$. And we do indeed have $\mathfrak{P}_2 \cap A = \wp_2$ because taking these quotients commutes with inclusions. □

Proposition 53
If B/A is an integral extension with $\mathfrak{P}$ and $\wp$ prime ideals of B and A respectively with $\mathfrak{P} \cap A = \wp$, then $\mathfrak{P}$ is maximal if and only if $\wp$ is maximal.

Proof. Again consider $\overline{A} = A/\wp$ and $\overline{B} = B/\mathfrak{P}$ as in the previous proof – we still have an inclusion $\overline{A} \hookrightarrow \overline{B}$, and $\overline{B}$ is integral over $\overline{A}$. We must prove that $\overline{A}$ is a field if and only if $\overline{B}$ is a field – **we'll drop the bars** from here on for notational convenience.

This proof only relies on the integrality of the extension and the fact that A and B are integral domains (since we mod out by a prime ideal). First of all, if A is a field and some nonzero $x \in B$ is integral over A, then $0 = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ for some n; we can divide this relation by powers of x until the constant term is nonzero because we have an integral domain. But then $-x(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1)/a_0 = 1$, so x is invertible. Thus B is a field since any nonzero element must be invertible. For the other direction, suppose A is not a field. Then there is some nonzero maximal ideal $\wp$, meaning that there is some prime ideal $\mathfrak{P}$ of B above $\wp$ which is also nonzero. But the only proper ideal of a field is the zero ideal, so B cannot be a field. □

The going-down theorem is similar but more subtle – we'll need an additional hypothesis:

Theorem 54 (Going down)
Let A and B be integral domains with A **integrally closed**. Suppose $\wp_1 \subseteq \wp_2$ are prime ideals of A and $\mathfrak{P}_2$ is a prime ideal of B above $\wp_2$. Then there exists a prime ideal $\mathfrak{P}_1$ of B such that $\mathfrak{P}_1 \subseteq \mathfrak{P}_2$ and $\mathfrak{P}_1$ lies above $\wp_1$.

In other words, we are trying to fill in a different corner of the diagram:

$$\begin{array}{ccc} \mathfrak{P}_1 & \subset & \mathfrak{P}_2 \\ \uparrow & & \uparrow \\ \wp_1 & \subset & \wp_2 \end{array}$$

We'll talk about the proof next time and show an illustrative example, and we'll just introduce an important concept here (and start next time with the proof of the subsequent result):

Definition 55

Let A be a domain, let $\mathfrak{a}$ be an ideal of A, and let $E \supset A$ be a field. An element $x \in E$ is **integral over $\mathfrak{a}$** if there is some equation $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ with $a_i \in \mathfrak{a}$.

Proposition 56

If A is an integrally closed integral domain with field of fractions F, E/F is a finite extension, and B is the integral closure of A in E, then $\{x \in B : x \text{ integral over } \mathfrak{a}\}$ is the radical $r(\mathfrak{a}B)$.

10 February 1, 2023

Last time, we proved the going-up theorem, which basically says that given $\wp_1 \subset \wp_2$ and $\mathfrak{P}_1$ lying over $\wp_1$, we can find a corresponding $\mathfrak{P}_2$ containing $\wp_1$ lying over $\wp_2$. And as we stated, the going-down theorem is similar but going from $\mathfrak{P}_2$ to $\mathfrak{P}_1$, and it requires an additional assumption.

Recall that if X is a variety (assume irreducible) over an algebraically closed field, so that $\mathcal{O}(X)$ is an integral domain, we can let K be its fraction field (which we also call the **function field** of X). Then the **dimension** of X is defined as the transcendence degree of K over F, and the **combinatorial dimension** is the d corresponding to any maximal chain of nonempty irreducible closed subspaces $X_0 \subseteq X_1 \subseteq \cdots \subseteq X_d$. But because we have a dictionary between irreducible closed subspaces and prime ideals of $\mathcal{O}(X)$ (which is an order-reversing bijection), this is the same as the **Krull dimension** of X, which is the corresponding d for a maximal length of a chain of prime ideals $0 = \wp_0 \subsetneq \wp_1 \subsetneq \cdots \subsetneq \wp_d$. But we can now make the final connection:

Theorem 57

Let X be a variety (a subspace of $\mathbb{F}^n$). Then the combinatorial dimension of X is the same as the dimension of X (with the definitions above).

Proof. First we will prove that $\mathcal{O}(X)$ has minimal nonzero prime ideals (in other words that we have some $\wp_1$, or equivalently that there are maximal proper irreducible subsets). Choose a transcendence basis $(y_1, \cdots, y_d)$ of K (where d is the dimension of X), so that $B = \mathcal{O}(X)$ is integral over $A = F[y_1, \cdots, y_d]$ (by Noether normalization). Since the y_is are algebraically independent, A is a polynomial ring and a unique factorization domain, and thus the minimal nonzero primes are (f) for some irreducible polynomial f. So in A we have $(0) \subset (f)$, so by the going-up theorem we have $(0) \subset \wp_1$ in B such that $\wp_1$ lies above (f). We claim that $\wp$ is a minimal prime ideal of B – indeed, we know that if B/A is integral and $\mathfrak{P}_1 \supseteq \mathfrak{P}_2$ are primes of B, then $\wp_1 = \mathfrak{P}_1 \cap A$ being the same as $\wp_2 = \mathfrak{P}_1 \cap \mathfrak{P}_2$ implies that $\mathfrak{P}_1 = \mathfrak{P}_2$. So we can't squeeze any other prime ideal between 0 and $\wp_1$, and furthermore any minimal prime of B arises in this way because intersecting it with A will yield some nonzero prime in A which is also minimal.

Now define $Y = V(\wp_1) \subset X$ be the corresponding maximal proper irreducible subset. We claim that $\dim(Y) = \dim(X) - 1$. Indeed, $\mathcal{O}(Y) = \mathcal{O}(X)/\wp_1$ is then integral over $F[\overline{y}_1, \cdots, \overline{y}_d] = F[y_1, \cdots, y_d]/(f)$, and (without loss of generality) the polynomial f must involves y_d, so $\overline{y}_d$ is algebraic over $F[\overline{y}_1, \cdots, \overline{y}_{d-1}]$. So the transcendence degree of the field of fractions of $\mathcal{O}(Y)$ is indeed less than d. But $\overline{y}_1, \cdots, \overline{y}_{d-1}$ are also algebraically independent, since any polynomial relation $g(\overline{y}_1, \cdots, \overline{y}_{d-1}) = 0$ corresponds to having $g \in F[y_1, \cdots, y_d]$ being in the kernel (f) of the quotient, and f involves y_d so this is not possible unless $g = 0$. So the transcendence degree indeed drops by one.

On the other hand, the combinatorial dimension of Y is also one less than the combinatorial dimension of X, because the images $\overline{\wp}_i$ of prime ideals $\wp_i \subseteq \mathcal{O}(X)$ in $\mathcal{O}(Y)$ will satisfy $0 = \overline{\wp}_1 \subsetneq \overline{\wp}_2 \subseteq \cdots \subsetneq \overline{\wp}_d$. And because every minimal prime ideal of $\mathcal{O}(X)$ arises this way, there's no other chain that is longer. So by induction this proves the result. □

We'll now talk more about the proof of the going-down theorem, where we should recall that we're filling in the top left corner of this diagram:

$$\begin{array}{ccc} \mathfrak{P}_1 & \subset & \mathfrak{P}_2 \\ \uparrow & & \uparrow \\ \wp_1 & \subset & \wp_2 \end{array}$$

Example 58

We do need the assumption that A is integrally closed for this result to hold. An instructive counterexample goes as follows: consider the curve $C = \{(x, y) : y^2 = x^2(x+1)\}$, which has a singularity at the origin.

As we've already discussed, $A = F[x, y : y^2 = x^2(x+1)]$ is not integrally closed, since $t = \frac{y}{x}$ is integral over A but not in A. Then $F[t]$ contains $F[x, y]$, since it contains $x = t^2 - 1$ and $y = t(t^2 - 1)$, so we have an integral extension $F[t]$ over $F[x, y]$. Then $F[t] = \mathcal{O}(D)$ is the coordinate ring for the affine line, and thus $F[x, y] \hookleftarrow F[t]$ corresponds to a morphism $\mathbb{A}^1 \to C$ which sends T to $(T^2 - 1, T(T^2 - 1))$ (so it finds the point on the curve of slope T). This map is not injective, since $T = \pm 1$ both map to the origin.

Remark 59. *More generally, we can prove (by looking at local rings) that for any curve C (meaning any variety of dimension 1), we have $\mathcal{O}(C)$ integrally closed if and only if C is nonsingular. Then the integral closure can be interpreted as $\mathcal{O}(D)$ for some other curve D, yielding a morphism $D \to C$ which resolves the singularities (meaning that the preimage of a singularity will come apart into several points). For higher-dimensional varieties, though, the integral closure might still be singular for a general algebraic surface. We then get a* **normal variety***, which is less singular, but it's still harder to work with and was only really done in the 1960s.*

So to get the counterexample we're looking for, consider the cylinder $C \times \mathbb{A}^1$, for which the function field is $F[x, y, z : y^2 = x^2(x+1)]$. This cylinder contains a similarly parameterized curve $z \mapsto (z^2 - 1, -z(z^2 - 1), z)$ which does not self-intersect but includes the two points $(0, 0, 1)$ and $(0, 0, -1)$ – let this curve be W. We thus have a mapping $\mathbb{A}^2 \to C \times \mathbb{A}^1$ given by

$$(T, Z) \mapsto (T^2 - 1, T(T^2 - 1), Z),$$

and this corresponds to $F[t, z]$ sitting above $F[x, y, z]$. The point now is that under this, $W' = \{(t, z) : t + z = 0\}$ will map to W.

Now the image of W is an irreducible curve, so W corresponds to some prime ideal $\wp_1$ in $F[x, y, z]$: specifically $\wp_1 = (xz + y, z^2 - 1 + x)$. That ideal corresponds above to the unique prime ideal $\mathfrak{P}_1 = (t + z)$ in $F[t, z]$. Then we

also have the maximal ideal $\wp_2 = (x, y, z-1)$, but there are two prime ideals of $F[t, z]$ that lie above this, namely $\mathfrak{P}_2 = (t-1, z-1)$ and $\mathfrak{P}_2' = (t+1, z-1)$. And now if we choose $\mathfrak{P}_2$, corresponding to a point not actually on W', then there is no $\mathfrak{P}_1$ that will satisfy the going-down theorem.

11 February 3, 2023

Last time, we showed that the going-down theorem does not always hold without the necessary assumption of being integrally closed. (We can take a look at the paper of Cohen and Seidenberg if we want more details – it's linked on the course website.) Thus, the statement we are instead trying to prove is that for any integral extension B/A with A an integrally closed integral domain, for any $\wp_1 \subset \wp_2$ prime ideals of A, and for any $\mathfrak{q}_2$ prime ideal of B above $\wp_2$ (**changing notation** here), there is some prime $\mathfrak{q}_1$ of B above $\wp_1$ with $\mathfrak{q}_1 \subset \mathfrak{q}_2$. Recall that the geometry of this setup is that if we have a dominant morphism $X \to Y$ with $A = \mathcal{O}(Y)$ and $B = \mathcal{O}(X)$, and we have varieties $V(\wp_2) \subset V(\wp_1)$ of Y, then if $V(\mathfrak{q}_2)$ maps to $V(\wp_2)$ we want to find a variety $V(\mathfrak{q}_1)$ containing it that maps to $V(\wp_1)$. And the point is that Y has to satisfy some additional conditions if we have the integrally closed suggestion – in the case where it's one-dimensional it's just saying that the curve is nonsingular.

To prepare for the proof, notice that if $\wp$ is a prime ideal of A (not necessarily maximal), then $A_\wp$ is a local ring which has a unique maximal ideal $\wp A_\wp$ and with $\wp A_\wp \cap A = \wp$. This has some useful applications:

Proposition 60
If B/A is an integral extension and $\wp$ is any prime ideal of A, then $\wp B \cap A = \wp$.

Note here that $\wp$ is not assumed to be maximal here, so $\wp B$ may not even be a prime ideal – for example if $A = \mathbb{Z}$ and $B = \mathbb{Z}[i]$, then $(3)B$ is maximal but not $(5)B$, since $(2+i)(2-i) = 5$. So instead $(5)B$ factors into a product of prime ideals (since we have a Dedekind domain).

Proof. By the Nakayama lemma, $\wp B$ is a proper ideal of B. We know that the prime ideals of $S^{-1}B$ are in bijection with the prime ideals of B that don't meet S (by applying intersection and extension). Applying this to $S = A - \wp$, we know that $A_\wp$ is a local ring, and $B_\wp = S^{-1}B$ is not necessarily a local ring but $\wp B$ does not meet S so it is contained in some maximal ideal $\mathcal{P}'$ of $B_\wp$. Then $\mathcal{P} = \mathcal{P}' \cap B$ is prime, and $\mathcal{P} \cap A = \mathcal{P}' \cap A_\wp \cap A \subset \wp A_\wp \cap A = \wp$. □

So the point is that passing to a local ring can allow us to make arguments of this type by taking advantage of the unique maximal ideal, and we're basically drawing the following picture:

$$\begin{array}{ccc} B & \longrightarrow & B_\wp = S^{-1}B \\ \uparrow & & \uparrow \\ A & \longrightarrow & A_\wp \end{array}$$

Here is another application:

Proposition 61
Let $\wp$ be a prime ideal of A, and suppose $A \subset B$ are rings (with B not necessarily integral over A). Assume that $\wp B \cap A = \wp$. Then there is some prime ideal of B above $\wp$.

Proof. Again look at a square as above. If we start with $\wp B$ in the top left corner, then we claim that $\wp B_\wp$ must be proper – indeed, if $1 = \sum p_i b_i / s_i$, then $\prod s_i$ woul dbe in $\wp B \cap A = \wp$, which is a contradiction. So $\wp B_\wp$ is

contained in some maximal ideal $\mathcal{P}'$ of $B_{\wp}$, and now as before let $\mathcal{P} = \mathcal{P}' \cap B$ be the prime ideal in B. Then $\mathcal{P} \cap A = \mathcal{P}' \cap A_{\wp} \cap A = \wp A_{\wp} \cap A = \wp$ because we have a local ring. $\square$

So the point is that localizing is magical because we can "pretend that ideals are maximal even if they aren't." We're now ready to return to the proof of going-down, starting by restating a definition and result from a previous lecture:

Definition 62

Let A be an integral domain, E be a field containing A ,and $\mathfrak{a}$ an ideal of A. We say that $x \in E$ is **integral over $\mathfrak{a}$** if it is the root of a monic polynomial with coefficients in $\mathfrak{a}$.

Proposition 63

Let B be integral over A, with field of fractions F, E for A, B respectively. Then $\{x \in B : x \text{ integral over } \mathfrak{a}\} = r(\mathfrak{a}B)$.

Proof. First we prove that if $x \in B$ is integral over A, then x is in the radical of $\mathfrak{a}B$. Indeed, we have

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0 \implies x^n = -\sum_i a_i x^i \in \mathfrak{a}B,$$

and thus x is in $r(\mathfrak{a}B)$. For the other direction, it **suffices to show that** elements of $\mathfrak{a}B$ are integral over $\mathfrak{a}$, because then if $x \in r(\mathfrak{a}B)$, then $x^n \in \mathfrak{a}B$ and thus x^n is integral over $\mathfrak{a}$ – the polynomial equation for which x^n is a root then also shows that there is a monic polynomial for which x is a root.

To do that, suppose $x \in \mathfrak{a}B$ – clearly this is true for $x = 0$, so we'll assume $x \neq 0$. We work with the ring $A[x^{-1}]$, and we define the ideal

$$\mathfrak{b} = \{y \in A[x^{-1}] : xy \in \mathfrak{a}A[x^{-1}]\}$$

If we can show that $\mathfrak{b}$ is not a proper ideal (so in fact $\mathfrak{b} = A[x^{-1}]$, then it must contain 1 and that will give us an integrality relation for x. Suppose otherwise, so that $\mathfrak{b}$ is contained in some maximal ideal $\mathfrak{m}$ of $A[x^{-1}]$. By the extension theorem, the homomorphism $A[x^{-1}] \to A[x^{-1}/\mathfrak{m}$ extends to a homomorphism $\Phi : V \to \overline{A[x^{-1}]/\mathfrak{m}}$, where V is a valuation ring of E containing $A[x^{-1}]$. Then $x \in V$, because $V \supset A$ and is integrally closed because it's a valuation ring, and $x \in B$ so it is integral over A. And $x^{-1} \in A[x^{-1} \subset V$, so both x and x^{-1} are in V. But then $\Phi(x^{-1}\mathfrak{a})$ maps to zero because we're extending a homomorphism that mods out by $\mathfrak{m}$, and $\Phi(x)$ is nonzero (because x is a unit in V), hence a unit, meaning that $\Phi(\mathfrak{a}) = 0$ as well, meaning $\Phi(\mathfrak{a}B) = 0$. But $x \in \mathfrak{a}B$ means that $\Phi(x) = 0$, which is a contradiction.

So $\mathfrak{b}$ is indeed all of $A[x^{-1}]$, hence containing 1, and in particular that means that means $x \in \mathfrak{a}A[x^{-1}]$ by definition of the ideal. Thus we have $x = a_0 + a_1x^{-1} + \cdots + a_nx^{-n}$ for some $a_i \in \mathfrak{a}$, and rearranging yields a monic polynomial showing that x is integral over $\mathfrak{a}$, as desired. $\square$

Proposition 64

Let A be integrally closed with field of fractions F, $E \supset F$ a field, and $\wp$ a prime ideal of A. Let $x \in E$ be integral over $\wp$, and suppose $x^n + a_{n-1}x^{n-1} + a_0$ be the (minimal) monic irreducible polynomial in $F[x]$. Then $a_i \in \wp$.

(The idea is that the polynomial showing integrality of x over $\wp$ may not be this irreducible one, but the irreducible one also has coefficients in $\wp$.)

Proof. Without loss of generality we may enlarge E and assume it contains all Galois conjugates α_i of x. If B is the integral closure of A in E, then $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ factors as $\prod_i (x - \alpha_i)$, with $\alpha_1 = x$ and potentially with repetition if the extension is not separable. But then the a_i are all in $r(\wp B) \subseteq r(\wp B \cap A) = r(\wp) = \wp$, as desired. □

We'll prove going-down using this result next time and then start dimension theory, including primary decomposition (and for more details we can read the book).

12 February 6, 2023

We'll start today by proving the going-down theorem. We'll use the notation mentioned last lecture, where we have $\wp_1 \subset \wp_2$ prime ideals in A and $\mathfrak{q}_2$ lying above $\wp_2$ in B (where B/A is an integral extension of integral domains, and A is integrally closed). Our goal is to show that we can find $\mathfrak{q}_1$ contained in $\mathfrak{q}_2$ and lying above $\wp_1$.

Proof. Let F and E be the field of fractions for A and B, respectively. Last time, we proved that if E/F is a finite extension of fields and A is an integral domain with field of fractions F, then if $x \in E$ is integral over some prime ideal $\wp$ of A (meaning that **some** monic polynomial with coefficients in $\wp$ has x as a root), then the **minimal** polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ of x over F also has coefficients in $\wp$. (The idea is that we can assume E/F is normal without loss of generality, and we can use that x being integral over $\wp$ is equivalent to having $x \in r(B\wp)$.)

To apply that to this theorem, first we'll prove that $\boxed{\wp_1 B_{\mathfrak{q}_2} \cap A = \wp_1}$. It is clear that $\wp_1 \subset \wp_1 B_{\mathfrak{q}_2} \cap A$. For the other direction, let $x \in \wp_1 B_{\mathfrak{q}_2} \cap A$, so that we can write $x = \frac{y}{s}$ for $y \in \wp_1 B$ and $s \in B - \mathfrak{q}_2$. By the criterion for integral dependence, since we know that $y \in \wp_1 B \subset r(\wp_1 B)$, we also know that y is integral over $\wp$, and thus the minimal polynomial $y^n + a_1 y^{n-1} + a_n = 0$ has all coefficients in $\wp_1$. Now because $s = \frac{y}{x}$, we have (dividing through by x^n)

$$s^n + b_1 s^{n-1} + \cdots + b_n = 0, \quad b_i = \frac{a_i}{x^i},$$

and (by our homework problem) these coefficients are also in A. But now if (for the sake of contradiction) x were not in $\wp_1$, then $a_i = x^i b_i$ is in $\wp$ but $x \notin \wp$, meaning $b_i \in \wp$ for all i. So then s would need to be integral over $\wp$, meaning that (again by the criterion for integral dependence) $s \in r(B\wp_1) \subset r(B\wp_2) \subset r(\mathfrak{q}_2) = \mathfrak{q}_2$ (last step because we have a prime ideal). This is a contradiction because s is in the complement of $\mathfrak{q}_2$. So in fact x must be in $\wp_1$ and the boxed equality is proved.

So now $\wp_1 B_{\mathfrak{q}_2}$ is contained in some prime ideal $\mathfrak{q}$ of $B_{\mathfrak{q}_2}$, and we may define $\mathfrak{q}_1 = \mathfrak{q} \cap B$. (So we start with $\wp_1$, extend it to $B_{\mathfrak{q}_2}$, and pull it back to B.) Here we're using the fact that if $\wp B \cap A = \wp$, then there is a prime of B above $\wp$ (via localizing). We know that $\mathfrak{q}_1$ does not meet $B - \mathfrak{q}_2$, since elements of the latter are units in $B_{\mathfrak{q}_2}$. This ideal then lies above $\mathfrak{p}_1$, so it is the desired one. □

We'll now begin our discussion of dimension theory, focusing on singularities (particularly of curves) and discrete valuation rings. We'll fix a ground field $\mathbb{F}$ which is algebraically closed.

Definition 65

Let $X \hookrightarrow \mathbb{A}^2$ be a plane curve, corresponding to some irreducible $f(X, Y) \in F[X, Y]$. A point $(a, b) \in X$ is **singular** if $\frac{\partial f}{\partial X}$ and $\frac{\partial f}{\partial Y}$ vanish at (a, b).

We've mentioned the example curve $f(X, Y) = Y^2 - X^2(X + 1)$ before, and we can indeed see that $(0, 0)$ is a singular point because there are no degree-1 terms.

Proposition 66

Any curve has only finitely many singular points.

Proof. The only way for $\frac{\partial f}{\partial X}$ and $\frac{\partial f}{\partial Y}$ to both be identically zero is if we're in characteristic p and all monomials have exponent a multiple of p, but it turns out that in that case we won't have an irreducible polynomial. Furthermore, if $\frac{\partial f}{\partial X}$ is nonzero, then it is not a multiple of f because f is irreducible. So we can eliminate one variable and see that $\frac{\partial f}{\partial X}$ and F can only have finitely many common zeros. □

Theorem 67

A point (a, b) is not a singularity if and only if the local ring $\mathcal{O}_{(a,b)}$ (of the coordinate ring $\mathcal{O}(X)$) is a discrete valuation ring.

Proof. We'll just prove the forward direction. We can assume without loss of generality by translation that $(a, b) = (0, 0)$. Since the point is not singular, we can't have both $\frac{\partial f}{\partial X}$ and $\frac{\partial f}{\partial Y}$ vanish, so we may assume without loss of generality that $\frac{\partial f}{\partial Y}(0, 0)$ is nonzero. We will show that the maximal ideal of this local ring is principal and generated by X; to do this, we'll show that if $g(X, Y)$ vanishes at $(0, 0)$ and if x, y are the images of X, Y in the coordinate ring (which is $F[x, y] \cong F[X, Y]/(f)$), then $g(x, y)$ is a multiple of x in the local ring. We know that $g(0, Y)$ vanishes at $Y = 0$, so we have $g(0, Y) = Yg_1(Y)$ for some polynomial $g_1 \in F[Y]$, and similarly we have $f(0, Y) = Yf_1(Y)$. If we now consider $f_1(Y)g(X, Y) - g_1(Y)f(X, Y)$, this polynomial vanishes when $X = 0$ because both terms are $Yf_1(Y)g_1(Y)$, so we have

$$f_1(Y)g(X, Y) - g_1(Y)f(X, Y) = Xh(X, Y).$$

Substituting in x, y for X, Y, we find that $f_1(y)g(x, y) = xh(x, y) \in (x)$ in the coordinate ring. But $f_1(y) \neq 0$ because $\frac{\partial f}{\partial Y}(0, 0)$ is nonzero by assumption (indeed, this comes from differentiating $f(0, Y) = Yf_1(Y)$ at $Y = 0$ and using the product rule), so $f_1(y)$ is a unit in $A_{(0,0)}$. Thus $g(x, y) = xh(x, y)f^{-1}(x, y)$ is indeed a multiple of x, as desired. There's a bit more work to showing that we do have a discrete valuation ring, but we can read up on that on our own. (There's a bit of Nakayama lemma involved, for example showing that if $\mathfrak{m}A_{\mathfrak{m}}$ is principal and generated by x, then $A_{\mathfrak{m}}$ is a discrete valuation ring.) □

We can now make the more general definition:

Definition 68

More generally, let A be an F-algebra of Krull dimension n. If $\mathfrak{m}$ is a maximal ideal, then the localization $A_{\mathfrak{m}}$ is a **regular local ring** if $\mathfrak{m}A_{\mathfrak{m}}$ can be generated by n elements. a variety is **nonsingular** at a point if the local ring at that point is a regular local ring.

For example, we have a local ring of dimension 1 in our case, and the ideal for the discrete valuation ring is generated by a single element. So for a curve, a necessary and sufficient condition is that we have a regular local ring of dimension 1, which is equivalent to having a discrete valuation ring by Theorem 67.

13 February 8, 2023

Primary decomposition is a necessary tool for dimension theory, so that's what our topic will be today. Recall that in a Dedekind domain, any nonzero ideal is of the form $\mathfrak{a} = \wp_1^{N_1} \cdots \wp_k^{N_k}$ for prime ideals $\wp_1, \cdots, \wp_k$. Assuming that the

$\wp_i$s are all distinct (so the repetition is encoded in the N_is), we then also have $\mathfrak{a} = \bigcap_i \wp_i^{N_i}$. The point of the primary decomposition is to generalize this fact to at least Noetherian rings.

Definition 69

Let A be a (commutative) ring. An ideal $\mathfrak{a}$ of A is **primary** if $xy \in \mathfrak{a}$ implies that either $x \in \mathfrak{a}$ or $y^n \in \mathfrak{a}$ for some n.

This condition may look a bit strange because it's not symmetric in x and y, but it does turn out to be a useful notion. The idea is that these primary ideals will take the role of the prime ideals in the Dedekind domain case.

Proposition 70

If $\mathfrak{a}$ is primary, then $r(\mathfrak{a}) = \{x \in A : x^n \in \mathfrak{a} \text{ for some } n\}$ is prime.

Proof. If $xy \in r(\mathfrak{a})$, then we know that $x^n y^n \in \mathfrak{a}$ for some integers m, n. This means that either $x^n \in \mathfrak{a}$ or $(y^n)^N \in \mathfrak{a}$ for some N, but in the former case $x \in r(\mathfrak{a})$ and in the latter $y \in r(\mathfrak{a})$. □

And notice that when we have $\mathfrak{a} = \wp_1^{N_1} \cdots \wp_k^{N_k}$ for prime $\wp_i$ in the Dedekind domain case, each $\wp_i^{N_i}$ is actually primary. So the analogous statement to show is that **for any Noetherian ring A, every ideal is a finite intersection of primary ideals**, and we'll be working towards that goal.

Definition 71

If $\mathfrak{a}$ is primary with corresponding prime ideal $\wp = r(\mathfrak{a})$, then we say that $\mathfrak{a}$ is **$\wp$-primary**.

Proposition 72

If $\mathfrak{q}_1, \mathfrak{q}_2$ are $\wp$-primary, then so is $\mathfrak{q}_1 \cap \mathfrak{q}_2$.

Proposition 73

Suppose that we have $xy \in \mathfrak{q}_1 \cap \mathfrak{q}_2$ but $x \notin \mathfrak{q}_1 \cap \mathfrak{q}_2$. Without loss of generality say that $x \notin \mathfrak{q}_1$, which means that $y \in r(\mathfrak{q}_1) = \wp$, which is also $r(\mathfrak{q}_2)$ by assumption. But this means that $y \in r(\mathfrak{q}_1 \cap \mathfrak{q}_2) = \wp$ (by taking a high enough power of y), as desired.

It is **not** true that $r(\mathfrak{a}) = \wp$ being prime implies that $\mathfrak{a}$ is primary, and we'll show an example in our homework. However, it is true that if $r(\mathfrak{a})$ is maximal, then $\mathfrak{a}$ is primary (also an exercise for us), and that implies the following result:

Proposition 74

Let A be noetherian. If $\mathfrak{m}$ is a maximal ideal, then an ideal $\mathfrak{a}$ is $\mathfrak{m}$-primary if and only if $\mathfrak{m} \supseteq \mathfrak{a} \supseteq \mathfrak{m}^n$ for some n.

Proof. For one direction, suppose $\mathfrak{a}$ is primary with $\mathfrak{a} \subset \mathfrak{m}$ and $r(\mathfrak{a}) = \mathfrak{m}$. Since $\mathfrak{m}$ is finitely generated, we may let $m = \langle x_1, \cdots, x_N \rangle$, and then $x_i^k \in \mathfrak{a}$ for all i for sufficiently large k. Then any element of $\mathfrak{m}$ is of the form $\sum a_i x_i$, and raising this to the Nk power yields a sum where all monomials have some degree-k power of one of the x_is, so $\mathfrak{m}^{Nk} \subseteq \mathfrak{a}$.

For the other direction, we use the exercise above: if $\mathfrak{m} \supseteq \mathfrak{a} \supseteq \mathfrak{m}^n$, then $\mathfrak{m} = r(\mathfrak{m})$ contains $r(\mathfrak{a})$, which contains $r(\mathfrak{m}^n) = \mathfrak{m}$. Thus $r(\mathfrak{a}) = \mathfrak{m}$ and thus $\mathfrak{a}$ is $\mathfrak{m}$-primary. □

Definition 75

A **primary decomposition** represents an ideal $\mathfrak{a}$ as a finite intersection of primary ideals $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \mathfrak{q}_r$.

If we group together (intersect) ideals that are primary with respect to the same prime, we may assume that all corresponding $\wp_i$ are distinct by Proposition 72 (meaning there is only one $\wp$-primary ideal of each $\wp$), and we may also assume that $\mathfrak{q}_i$ is not contained in $\bigcap_{j \neq i} \mathfrak{q}_j$ (or else we could just throw away $\mathfrak{q}_i$). Then the minimal prime ideals $\mathfrak{p}_i = r(\mathfrak{q}_i)$ that appear are unique, but overall this decomposition may still not be unique:

Example 76

Consider the polynomial ring $F[X, Y]$. Then we claim $(X) \cap (X^2, XY, Y^2)$ is the same ideal as $(X) \cap (X^2, Y)$.

Indeed, (X^2, Y) is clearly contained in (X^2, XY, Y^2). On the other hand, an element α of (X^2, XY, Y^2) is any polynomial whose monomials all have degree at least 2, so the intersection $(X) \cap (X^2, XY, Y^2)$ is a sum of monomials $a_{ij}X^iY^j$ with $i + j \geq 2$ and $i \neq 0$ – thus it is also a monomial in (X^2, Y). But now $r(X^2, XY, Y^2) = r(X^2, Y) = (X, Y)$ is a maximal ideal, and (X) is prime, so everything here is primary. So the uniqueness does hold at the level of the primes, but not at the level of primary ideals. And now we'll show existence:

Theorem 77

In a noetherian ring A, any ideal is the intersection of primary ideals.

Proof. Call an ideal **irreducible** if it is not the finite intersection of two larger ideals (that is, if $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$, then either $\mathfrak{a} = \mathfrak{b}$ or $\mathfrak{a} = \mathfrak{c}$). First note that every ideal is an intersection of irreducible ideals by a Zorn's lemma argument. Indeed, if there is some ideal with no irreducible decomposition, then choose a maximal such counterexample (here we use Noetherianness). Then $\mathfrak{a}$ is not irreducible, so we can write $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ with $\mathfrak{b}, \mathfrak{c}$ larger, meaning that each of them is an intersection of irreducibles. But this gives us a way to write $\mathfrak{a}$ as an intersection of irreducibles, which is a contradiction.

So now it suffices to show that every irreducible ideal is actually primary. Let $\mathfrak{a}$ be irreducible, and let $\overline{A} = A/\mathfrak{a}$, so that the zero ideal is not the intersection of nonzero ideals. We'll drop the bars in the notation and just prove that for any ring where 0 is not the intersection of two nonzero ideals, the ideal (0) is primary (in other words, zero divisors are nilpotent). Indeed, (0) being primary in $\overline{A}$ is exactly the same condition as $\mathfrak{a}$ being primary in A.

Suppose that $xy = 0$ but $x \neq 0$; we wish to show that $y^n = 0$ for some n. Define the ideals

$$\mathfrak{a}_n = \{z \in A : zy^n = 0\}.$$

If z annihilates y^n, then it annihilates y^{n+1} as well, so $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$, so by the ascending chain condition we have $\mathfrak{a}_N = \mathfrak{a}_{N+1}$ for some N. In other words, $zy^{N+1} = 0$ implies that $zy^N = 0$. We claim that $y^N = 0$; suppose otherwise. Then (x) and (y^N) are both nonzero ideals, so $(x) \cap (y^N)$ is not the zero ideal and the intersection contains some $a \in A$. Then $a = z_1x = z_2y^N$ for some $z_1, z_2 \in A$, so

$$0 = z_1xy = ay = y^{N+1}z_2 \implies a = y^Nz_2 = 0,$$

which is a contradiction. Thus irreducible ideals are indeed primary and we always have a finite decomposition. □

14 February 10, 2023

Today's topics are the **Hilbert polynomial and the statement of the dimension theorem**, which is the equivalence of three different definitions of dimension for rings in algebraic geometry (due to Krull). A good reference for this material is the set of lecture notes on the website or the last chapter of Atiyah and Macdonald.

Definition 78

A **graded ring** is a ring $G = \bigoplus_{i=0}^{\infty} G_i$ in which G_0 is a ring, each G_i is a G_0 abelian group module, the multiplication respects the grading (meaning that $G_i G_j \subseteq G_{i+j}$) and is bilinear and associative.

Here, G_0 will be a ring, and its unit will be a unit for the entire graded ring. But the higher G_is don't necessarily have to be rings anymore (in particular they are not closed under multiplication). We often take $G_0 = F$ a field and G_i abelian group modules for G_0.

Example 79

A polynomial ring is graded by degree, and more generally we can often replace an affine algebra by a related graded ring. For example, if we take $y^2 = x(x^2 - 1)$, which is an elliptic curve, then the complex points on this curve actually form a torus with a point missing (which is the "point at infinity").

To recover this point at infinity, we can make the equation homogeneous by adding appropriate powers of an extra variable z, so that the equation becomes $y^2 z = x^3 - xz^2$. We can now think of (x, y, z) as projective coordinates, meaning we identify (x, y, z) with $(\lambda x, \lambda y, \lambda z)$ for any nonzero λ; that is, we define

$$\mathbb{P}^2 = \{(x, y, z) \text{not all zero} : (x, y, z) = (\lambda x, \lambda y, \lambda z) \text{ for all } \lambda \neq 0\}.$$

This contains $\mathbb{A}^2 = \{(x, y, 1)\}$, so most of the points in $\mathbb{P}^2$ are the ones in $\mathbb{A}^2$. But there's also an additional line at infinity of points of the form $(x, y, 0)$, and out of these the point $(0, 1, 0)$ is on our elliptic curve. And now the polynomial $f(x, y, z) = y^2 z - x^3 + xz^2$ is homogeneous of degree 3, and that allows us to associate to this elliptic curve the graded ring of the **projective variety** $\mathbb{F}[X, Y, Z]/(f)$, with grading again given by degree.

The idea is that when $G = \bigoplus_i G_i$, then the elements within a given G_i are called **homogeneous** of degree i, and those are the ones that actually have meaning in the algebraic geometry sense here. (But we should think of them as sections of a line bundle instead of as functions.)

Example 80

Let A be a commutative ring and $\mathfrak{a}$ an ideal (which we should think of as being maximal). Then set $G_0 = A/\mathfrak{a}$ and $G_i = \mathfrak{a}^i/\mathfrak{a}^{i+1}$ for all $i > 0$.

To check that this gives us a graded ring, we must check that multiplication respects the grading. Specifically, we should check that the multiplication map induces a map $\mathfrak{a}^i \oplus \mathfrak{a}^j \to \mathfrak{a}^{i+j}$, and that $(\mathfrak{a}^{i+1}, 0)$ and $(0, \mathfrak{a}^{i+j+1})$ map into $\mathfrak{a}^{i+j+1}$, so that we get an induced map $\mathfrak{a}^i/\mathfrak{a}^{i+1} \times \mathfrak{a}^j/\mathfrak{a}^{j+1} \to \mathfrak{a}^{i+j}/\mathfrak{a}^{i+j+1}$ by the universal property of the quotient.

Definition 81

Let $G = \bigoplus_i G_i$ be a Noetherian graded ring, and assume that G_0 is a field. A **graded module** of G is a module $M = \bigoplus_i M_i$ such that $G_i M_j \subseteq M_{i+j}$.

In particular, G is a graded module over itself.

Definition 82

For M a graded module of G (where G_0 is a field), the **Hilbert series** of M is $P_M(t) = \sum_{i=0}^{\infty} \dim_{G_0}(M_i)t^i$.

Theorem 83

Let G be a graded Noetherian ring. Suppose G is generated as an algebra by $X_1, \cdots, X_n$, where each X_i is homogeneous of degree d_i (meaning that $X_i \in G_{d_i}$). Then for any finitely generated graded module M of G, we have

$$P_M(t) = \frac{f(t)}{(1-t^{d_1})\cdots(1-t^{d_n})}$$

for some polynomial $f(t)$.

Proof. We will assume G_0 is a field – the case where G_0 is not a field we'll do later on. We induct on the number of generators n – the base case $n = 0$ is true because $G = \mathbb{F}$ and we just have a finite-dimensional vector space. Notice that $G_0' = F[x_1, \cdots, X_{n-1}]$ is also a graded ring, and M can also be thought of as a G_0'-module. Consider the multiplication map $M_i \to M_{i+d_n}$ given by multiplication by x_n. Defining $Q = M/X_nM$, the map $M_{i+dn} \to Q_{i+dn}$ is surjective, so we have an exact sequence

$$0 \to K_i \to M_i \to M_{i+d_n} \to Q_{i+d_n} \to 0$$

where K_i is the kernel of the multiplication-by-X_n map in M_i. We claim that this means

$$\dim(K_i) - \dim(M_i) + \dim(M_{i+d_n}) - \dim(Q_{i+d_n}) = 0$$

(we can do this by introducing another term in the short exact sequence with $0 \to K_i \to M_i \to A_i \to 0$ and $0 \to A_i \to M_{i+d_i} \to Q_{i+d_n} \to 0$). Multiplying this equation by t^{i+d_n} and summing over i (starting from $-d_n$; here we're defining the dimension of M_i to be zero for $i < 0$ and that still makes the equation hold), we find that

$$t^{d_n}P_K(t) - t^{d_n}P_M(t) + P_M(t) - P_Q(t) = 0,$$

and rearranging this shows that $P_M(t) = \frac{P_Q(t) - t^{d_n}P_K(t)}{1-t^{d_n}}$. But Q and K are both annihilated by x_n, and this same result holds whether we regard them as G-modules or G'-modules. So by the inductive hypothesis both of those terms are $\frac{1}{(1-t^{d_1})\cdots(1-t^{d_{n-1}})}$ times a polynomial. Plugging that in yields the result. □

Suppose A is a Noetherian ring and $\mathfrak{m}$ is a maximal ideal of A. We then have $G = G_{\mathfrak{m}} = \bigoplus_{i=0}^{\infty}(\mathfrak{m}^i/\mathfrak{m}^{i+1})$, and $G_1 = \mathfrak{m}/\mathfrak{m}^2$ is then important in connection with singularities and the Zariski tangent space, which we can read about on our own.

Theorem 84

There is a polynomial $\chi_m(k)$ such that for all sufficiently large k, the length $\ell(A/\mathfrak{m}^k)$ of a module is equal to $\chi_m(k)$.

The idea is that $A/\mathfrak{m}^k$ might not be a vector space even though $\mathfrak{m}^{k-1}/\mathfrak{m}^k$ is, so we need this more general definition:

Definition 85

Suppose a module M has a composition series $0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_d = M$, where all M_i/M_{i-1} are simple modules (that is, they have no nonzero proper submodules). By Jordan-Hölder (proof is identical as the one for groups), all such series have the same length and quotients up to ordering. The **length** of M is then the value of d (or ∞ if not).

If we have a short exact sequence $0 \to M' \to M \to M'' \to 0$, we can put the composition series for M' and M'' together and get one for M, so $\ell(M) = \ell(M') + \ell(M'')$. We'll prove this last result about the Hilbert polynomial next time!

15 February 13, 2023

Our goal today is to state the Krull dimension theorem (showing equivalence of several definitions of dimension). Recall that we previously defined the Hilbert series of a graded module M of a graded ring G (currently defining only when G_0 is a field) to be $P_M(t) = \sum_{i=0}^{\infty} \dim_{G_0}(M_i)t^i$ (where the gradedness here means that $G = \bigoplus G_i$ and $M = \bigoplus M_i$ with $G_iG_j \subset G_{i+j}$ and $G_iM_j \subset M_{i+j}$). Furthermore, we proved that if G is noetherian and finitely generated by homogeneous elements of degree d_i, and M is finitely generated, then $P_M(t)$ is a polynomial times $\frac{1}{(1-t^{d_1})\cdots(1-t^{d_n})}$.

We then mentioned one way of constructing graded rings: let A be a noetherian local ring with maximal ideal $\mathfrak{m}$. Then may define

$$G_{\mathfrak{m}} = \bigoplus_{k=0}^{\infty} (\mathfrak{m}^k/\mathfrak{m}^{k+1}),$$

where the degree-0 part $G_{\mathfrak{m},0} = \mathfrak{m}^0/\mathfrak{m} = A/\mathfrak{m}$ is a field. Then the multiplication in the ring $\mathfrak{m}^k \times \mathfrak{m}^\ell \to \mathfrak{m}^{k+\ell}$ induces a multiplication $G_{\mathfrak{m},k} \times G_{\mathfrak{m},\ell} \to G_{\mathfrak{m},k+\ell}$, so we do get a noetherian graded ring. In fact, this ring is generated by elements of degree 1 (that is, by $\mathfrak{m}/\mathfrak{m}^2$).

Lemma 86

If $X_1, \cdots, X_n$ generate $\mathfrak{m}/\mathfrak{m}^2$ as a vector space over $F = A/\mathfrak{m}$, then they generate $\mathfrak{m}$ as an ideal.

Proof. This is basically a Nakayama's lemma argument. Consider the submodule $\mathfrak{m}'$ of $\mathfrak{m}$ generated by $X_1, \cdots, X_n$. Since we generate $\mathfrak{m}/\mathfrak{m}^2$ as a vector space, $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}^2$ (since anything in $\mathfrak{m}$ can be expressed as a linear combination $\sum_i c_iX_i$ with $c_i \in A$, plus some correction term $\phi \in \mathfrak{m}^2$. Then multiplying any such element by $\mathfrak{m}$ makes everything on the right-hand side in $\mathfrak{m}^2$. But then $\mathfrak{m}$ annihilates $\mathfrak{m}/\mathfrak{m}'$, so by Nakayama's lemma this means $\mathfrak{m}/\mathfrak{m}' = 0$ and thus $\mathfrak{m} = \mathfrak{m}'$. (Here we do need that A is local.) □

If we now apply the same proof to the case $G_{\mathfrak{m}} = \bigoplus_{k=0}^{\infty} G_{\mathfrak{m},k}$ with $G_{\mathfrak{m},k} = \mathfrak{m}^k/\mathfrak{m}^{k+1}$, then a basis of $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ yields a set of generators of $\mathfrak{m}^k$. Furthermore, if we take the dual space of $(\mathfrak{m}/\mathfrak{m}^2)$, we will get the **Zariski tangent space** at a point a if A is a local ring, and thus a variety of X at $\mathfrak{a}$. The intuitive understanding (which does hold for curves) is that if X has dimension d, then the dimension of $\mathfrak{m}/\mathfrak{m}^2$ as a vector space (where the maximal ideal corresponds to some point a) is at least d and is exactly d when X is not singular at a. For example, for the curve $y^2 = x^2(x+1)$, we see that $\dim(\mathfrak{m}/\mathfrak{m}^2) = 2$ at the origin because of the intersection point, but $\dim(X) = 1$.

Definition 87

For a local ring A with maximal ideal $\mathfrak{m}$, let $\delta(A)$ be the minimum number of generators needed for an $\mathfrak{m}$-primary ideal of A.

Remember that $\mathfrak{q}$ is $\mathfrak{m}$-primary if and only if $\mathfrak{m} \supseteq \mathfrak{q} \supseteq \mathfrak{m}^n$ for some n, and in this case we claim that the ideal $\mathfrak{q} = (x)$ is $\mathfrak{m}$-primary because $y^2 = x^2(x+1) \subset \mathfrak{q}$, meaning all of $\mathfrak{m}^2 = (x,y)^2 = (x^2, xy, y^2)$ is contained in $\mathfrak{q} = (x)$. But then because $\mathfrak{q}$ is generated by just a single element, $\delta(A) = 1$ but $\dim(\mathfrak{m}/\mathfrak{m}^2) = 2$ – the point is that we may want to look at other ideals besides just $\mathfrak{m}$ itself.

Since $G_{\mathfrak{m}}$ is generated by elements of degree 1, its Hilbert polynomial then has the form $\frac{f(t)}{(1-t)^d}$, where $d = \dim(\mathfrak{m}/\mathfrak{m}^2)$. We can look at the power series expansion

$$\frac{1}{(1-t)^d} = \sum_{k=0}^{\infty} C(d,k)t^k,$$

where $C(d,k) = \binom{d+k-1}{d-1}$ is a binomial coefficient (specifically, a degree $(d-1)$ polynomial in k). Last time, we stated that there is a polynomial $\chi_m(k)$ such that for all sufficiently large k, $\chi_m(k) = \ell(A/\mathfrak{m}^k)$ is the length of the module $A/\mathfrak{m}^k$ (that is, the number of factors in its composition series). In particular, if M is semisimple (for instance since $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ is a vector space, this is just the dimension of M). This is called the **Hilbert-Samuel polynomial**, and a key fact is that the **length agrees with the dimension** (and thus the corresponding Hilbert series) when we have a semisimple module, for example if $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ is a vector space. Furthermore, the length has the nice property that $\ell(M') = \ell(M) + \ell(M'')$ for a short exact sequence $0 \to M \to M' \to M'' \to 0$. However, $A/\mathfrak{m}^k$ may not be a vector space and thus its dimension does not make sense in general (this is why we need to use length instead).

Proof of existence of Hilbert-Samuel polynomial. We claim that

$$\boxed{\ell(A/\mathfrak{m}^k) = \sum_{i=0}^{k-1} \dim(\mathfrak{m}^i/\mathfrak{m}^{i+1})},$$

since we can calculate length inductively via the short exact sequence $0 \to \mathfrak{m}^k/\mathfrak{m}^{k+1} \to A/\mathfrak{m}^{k+1} \to A/\mathfrak{m}^k \to 0$. This then means that $\ell(A/\mathfrak{m}^k) = \sum_{i=0}^{k-1} \dim G_{\mathfrak{m},i}$, and we can combine this with the expression for the Hilbert polynomial $\sum \dim(G_{\mathfrak{m},k})t^k = \frac{f(t)}{\prod(1-t_i^d)}$. Specifically, if the numerator is of the form $f(t) = \sum c_j t^j$, then the series expansion above tells us that

$$\dim(G_{\mathfrak{m},k}) = \sum_j c_j \binom{k-j+d-1}{k-j} = \sum_j c_j \binom{k-j+d-1}{d-1}$$

is a polynomial in k of degree at most $(d-1)$ since each term is of degree at most $(d-1)$, as long as k is large enough (larger than the degree of f). Now accumulating within the boxed equation above makes $\ell(A/\mathfrak{m}^k)$ a polynomial as well (here we're saying that if $p(x)$ is a degree $(d-1)$ polynomial, then the cumulative sums $p(1) + \cdots + p(x)$ yield a degree d polynomial). □

This proof may not be very satisfying because it is not specific enough to show a direct connection, but next time, we'll prove the dimension theorem. The statement is that if A is a noetherian local ring, then the following are equal: (1) $\delta(A)$ as defined today, (2) the actual degree of χ_m, and (3) the dimension of A. The proof is nice – it basically involves proving the circular implications, each using a different technique.

16 February 15, 2023

Since we're slightly behind schedule with lectures, we'll start the proof of the dimension theorem today, then discuss group representation theory next lecture, and then return to the dimension theorem next week.

Theorem 88

Let A be a noetherian local ring with maximal ideal $\mathfrak{m}$. Let $d(A)$ be the degree of the Hilbert-Samuel polynomial, $\delta(A)$ be the smallest number of generators in an $\mathfrak{m}$-primary ideal of A, and $\dim(A)$ be the Krull dimension of A (the shortest length of a saturated chain of prime ideals). Then $d(A) = \delta(A) = \dim(A)$.

Recall that part of the magic here is that some $\mathfrak{m}$-primary ideal will have fewer generators than $\mathfrak{m}$ itself if the coordinate ring corresponding to $\mathfrak{m}$ is not a regular local ring (that is, a local ring of a singular point). And remember that we've already shown $\dim(A)$ is equivalent to the transcendence degree of the fraction field for the corresponding coordinate ring.

We will first prove that **(1)** $d(A) \leq \delta(A)$. We have already almost finished proving that $d(A)$ is at most the number of generators of $\mathfrak{m}$, but we need something stronger (in case some $\mathfrak{m}$-primary ideal has fewer generators).

Let's first explain that weaker statement. Let $G_{\mathfrak{m}}$ be the graded ring $\bigoplus G_{\mathfrak{m},i}$, where $G_{\mathfrak{m},i} = \mathfrak{m}^i/\mathfrak{m}^{i+1}$ and $G_{\mathfrak{m},0} = A/\mathfrak{m} = F$ is our ground field. Recall that the Hilbert-Samuel polynomial satisfies $\chi_{\mathfrak{m}}(k) = \ell(A/\mathfrak{m}^k)$ as long as k is at least the degree of the largest generator of the graded $G_{\mathfrak{m}}$, and it is actually a polynomial. Indeed, remember that the Hilbert series $P_{G_{\mathfrak{m}}}(t) = \sum_{i=0}^{\infty} \ell(\mathfrak{m}^i/\mathfrak{m}^{i+1})t^i$ is of the form $\frac{g(t)}{(1-t^{d_1})\cdots(1-t^{d_r})}$ if G is generated as an F-algebra by $x_1, \cdots, x_r$ with $x_i \in G_{\mathfrak{m},i}$ with degree $d_1, \cdots, d_r$. But $G_{\mathfrak{m}}$ is generated by elements of $\mathfrak{m}/\mathfrak{m}^2$ (that is, elements of degree 1), we in fact have Hilbert series $\frac{g(t)}{(1-t)^r}$. Using that $\frac{1}{(1-t)^r} = \sum \binom{r+i-1}{r-1} t^i$, which has coefficients of degree $r-1$ (in i), and that $\chi_{\mathfrak{m}}(k) = \sum_{i<k} \ell(\mathfrak{m}^i/\mathfrak{m}^{i+1})$, the accumulation must have at most degree r. But in fact the degree can be less than r because of potential cancellations:

Example 89

Let $\mathfrak{m}$ be the local ring of $y^2 = x^3$ at the origin $(0,0)$. Then $\ell(\mathfrak{m}^i/\mathfrak{m}^{i+1})$ is 1 if $i = 0$ and 2 if $i \geq 1$, but the Hilbert-Samuel polynomial is $\chi_{\mathfrak{m}}(k) = 2k+1$, which has degree 1. The idea is that in the expression of $P_{G_{\mathfrak{m}}}(t) = \frac{1-t^2}{(1-t)^2}$, we can in fact cancel a power of $1-t$ in the denominator.

So we're now going to go into the proof more carefully but working with an $\mathfrak{m}$-primary ideal.

Proof that $d(A) \leq \delta(A)$. Recall that if $\mathfrak{q}$ is an $\mathfrak{m}$-primary ideal, then $\mathfrak{m} \supseteq \mathfrak{q} \supseteq \mathfrak{m}^n$ for some n. Define the graded ring

$$G_{\mathfrak{q}} = \bigoplus G_{\mathfrak{q},i}, \quad G_{\mathfrak{q},i} = \mathfrak{q}^i/\mathfrak{q}^{i+1},$$

where $G_{\mathfrak{q},0} = A/\mathfrak{q}$ is no longer a field and thus we must use length in the definition of

$$P_{G_{\mathfrak{q}}} = \ell(\mathfrak{q}^i/\mathfrak{q}^{i+1})t^i.$$

But the same theory goes through with this new definition, and now $\chi_{\mathfrak{q}}(k) = \ell(A/\mathfrak{q}^k)$ will be a polynomial of degree at most the number of generators s needed for $\mathfrak{q}$. Note that an element thought of as an element of $G_{\mathfrak{m}}$ or of $G_{\mathfrak{q}}$ may be of different degrees, but since $\mathfrak{m} \supseteq \mathfrak{q} \supseteq \mathfrak{m}^n$ we know that $\mathfrak{m}^k \supseteq \mathfrak{q}^k \supseteq \mathfrak{m}^{nk}$ – in particular $\ell(A/\mathfrak{m}^k) \leq \ell(A/\mathfrak{q}^k) \leq \ell(A/\mathfrak{m}^{nk})$ means that $\chi_{\mathfrak{m}}(k) \leq \chi_{\mathfrak{q}}(k) \leq \chi_{\mathfrak{m}}(Nk)$, which can only happen if in fact the degrees of $\chi_{\mathfrak{m}}$ and $\chi_{\mathfrak{q}}$ are the same. So the degree of $\chi_{\mathfrak{m}}$ is in fact at most the number of generators needed for $\mathfrak{q}$ as well. □

Next, we'll show that $\delta(A)$ is at most the Krull dimension, which will use some properties of the primary decomposition:

Proposition 90

Let A be a noetherian ring, $\mathfrak{a}$ be an ideal, and $\mathfrak{a} = \bigcap_{i=1}^{N} \mathfrak{q}_i$ be a primary decomposition of $\mathfrak{a}$. Let $\wp_i = r(\mathfrak{q}_i)$ be the associated primes for the primary ideals. Then any prime ideal containing $\mathfrak{a}$ contains some $\wp_i$.

Proof. Notice that if $\wp \supseteq \mathfrak{a}$, then $\wp \supseteq \mathfrak{q}_i$ for some i; otherwise let $x_i \in \mathfrak{q}_i \setminus \wp$ and notice that $\prod x_i \in \bigcap \mathfrak{q}_i = \mathfrak{a}$ but no x_i is in $\wp$. So $\wp = r(\wp)$ contains $r(\mathfrak{q}_i) = \wp_i$. □

(Basically, even though the $\mathfrak{q}_i$s are not canonical, the minimal primes are uniquely determined, and containment does reflect this fact.)

Proposition 91

Let $\mathfrak{a}$ be an ideal and $\wp_i$ prime ideals of A. If $\mathfrak{a} \subset \bigcup_{i=1}^{N} \wp_i$ (note that this is not the ideal formed by all of the $\wp_i$s), then $\mathfrak{a} \subset \wp_i$ for some i.

Proof. We prove this by induction on N. The base case $N = 1$ is clear, and now assume the statement holds for $N - 1$. Suppose for the sake of contradiction that $\mathfrak{a} \subset \bigcup_{i=1}^{N} \wp_i$ but $\mathfrak{a}$ is not contained in any $\wp_i$. Then for any fixed index i there is $x_i \in \mathfrak{a} \setminus \bigcup_{j \neq i} \wp_j$ (here we've used the inductive hypothesis). But since $\mathfrak{a}$ is contained in the union of all $\wp_j$s, that means $x_i \in \wp_i$. Then the element

$$x = \sum_j \prod_{i \neq j} x_i$$

is in $\mathfrak{a}$ because each x_i is in $\mathfrak{a}$, so $x \in \wp_k$ for some k. But now all terms except the one where $j = k$ have a copy of x_k, so all terms except $\prod_{i \neq k} x_i$ are in $\wp_k$, meaning $\prod_{i \neq k} x_i$ must be in $\wp_k$ as well. But no component is in $\wp_k$, contradicting primeness of $\wp_k$. Thus the inductive hypothesis is proved. □

Definition 92

The **height** of a prime ideal $\wp$ is the maximal k corresponding to a chain of primes $\wp_0 \subsetneq \wp_1 \subsetneq \cdots \subsetneq \wp_k = \wp$.

In particular, the height of a maximal ideal $\mathfrak{m}$ is exactly the Krull dimension $\dim(A)$ (since every chain ends with a maximal ideal).

Proposition 93

Suppose A is a local noetherian ring. Then there is a chain of elements $x_1, \cdots, x_r$ of $\mathfrak{m}$ such that any ideal containing $(x_1, \cdots, x_i)$ has height at least i and such that $(x_1, \cdots, x_r)$ is $\mathfrak{m}$-primary.

In particular, this means that $\dim(A) = \text{height}(\mathfrak{m}) \geq r$, which is the number of generators needed for the particular $\mathfrak{m}$-primary ideal $(x_1, \cdots, x_r)$. So this implies that $\delta(A) \leq \dim(A)$.

Proof. Assume $x_1, \cdots, x_i$ have already been constructed. If $r(x_1, \cdots, x_i) = \mathfrak{m}$, then we're done; otherwise $(x_1, \cdots, x_i)$ is not $\mathfrak{m}$-primary. There are a finite number of minimal primes containing $(x_1, \cdots, x_i)$ (by using the primary decomposition and Proposition 90), each of which is a proper subideals of $\mathfrak{m}$. Since $\mathfrak{m}$ is not the union of these minimal primes, we can then find some $x_{i+1} \in \mathfrak{m}$ not in any of them. Now if $\wp$ is a prime containing $(x_1, \cdots, x_i)$, its height is

at least i by the inductive hypothesis, and now if it also contains x_{i+1} its height must be bigger than i (since it is not among the minimal primes containing $(x_1, \cdots, x_i)$), which is what we wanted to show. And we finish when we get a $\mathfrak{m}$-primary ideal with radical equal to $\mathfrak{m}$. □

The last part of the proof of the dimension theorem requires the Artin-Rees lemma, which we'll show on our homework. And we'll discuss that last part in the lecture after the next one.

17 February 17, 2023

We'll discuss semisimplicity today, for which the most relevant example comes from group representation theory.

Definition 94

Let G be a finite group. A **representation** of G is a homomorphism $\pi : G \to \mathrm{GL}(V)$ for some vector space V (usually in this class over $\mathbb{C}$ and usually finite dimensional).

There is a branch of representation theory in which V is of positive characteristic (say p) where p is a prime dividing the order of the group G. This is called modular representation theory, which can get information that can't be obtained otherwise, but it's outside the scope of this course. So we will avoid that here and just work over $\mathbb{C}$, since that gives us the same information as any characteristic p not dividing the order of G and it's good to work over an algebraically closed field.

Definition 95

Let F be a field and G be a finite group. The **group algebra** $F[G]$ is the free vector space on G, which is the set of formal summations $\sum_{g \in G} a_g g$ with $a_g \in F$.

In particular, $F[G]$ has a ring structure given by

$$\left(\sum a_g \cdot g\right)\left(\sum b_g \cdot g\right) = \sum c_g \cdot g, \quad c_g = \sum_{x,y:xy=g} a_x b_y$$

(in other words, extend the group multiplication by linearity), and it is commutative if and only if G is abelian. (So in particular we now have to introduce **noncommutative rings** into the class.)

Theorem 96 (Maschke)

If F is a field of characteristic zero, or of characteristic p with p not dividing $|G|$, then $F[G]$ is a **semisimple** group algebra.

Before we define what semisimplicity is, we'll first establish a relationship between representations and modules over the group algebra:

Theorem 97

There is a bijection between representations of G on F-vector spaces and left modules over $F[G]$.

This bijection is given as follows: given $\pi : G \to \mathrm{GL}(V)$, we can define the $F[G]$ module structure given by

$$(\sum a_g \cdot g)v = \sum a_g \pi(g) v.$$

So the point is that π is a homomorphism exactly when this gives us a module structure – we need to check that if ξ, η are in the group algebra, then $\zeta(\eta v) = (\zeta\eta)v$, but that reduces by linearity to the case where $\zeta, \eta \in G$, and having $\pi(\xi)(\pi(m)g) = \pi(\xi\eta)g$ is equivalent to having $\pi(\xi)\pi(\eta) = \pi(\xi\eta)$. And if we have a module V, we may define $\pi : G \to \mathrm{GL}(V)$ by mapping $gv = (\pi(g))v$, and these constructions are inverses of each other. Sometimes we say that V is a **G-module** instead of saying that it is an $F[G]$-module.

We may ask whether this vector space V has **invariant subspaces**, meaning that we have a subspace $W \subseteq V$ with $\pi(g)W \subseteq W$ for all $g \in G$. (Being invariant under the group then means we are invariant as a submodule of V regarded as an $F[G]$-module, so we can think of it that way as well.) In particular this also means $\pi(g^{-1})W \subseteq W$ and thus we must have $\pi(g)W = W$.

Definition 98

A vector space V is **irreducible** as a G-module if 0 and V are the only invariant subspaces.

We will prove soon that there are only finitely many isomorphism classes of such irreducibles for any G.

Definition 99

For any ring R, a left R-module M is **simple** if the only submodules of M are 0 and M.

So in particular, V is irreducible if and only if it is simple as an $F[G]$-module, so these terms are almost synonymous.

Proposition 100

Let R be a (not necessarily commutative) ring and M an R-module, possibly infinite-dimensional. Then the following are equivalent:

1. M is a sum of simple submodules,
2. M is a direct sum of simple submodules,
3. (Complete reducibility) For any $N \subseteq M$, there is some submodule P (not necessarily unique) with $M = N \oplus P$. (We say that N is **complemented**.)

A module satisfying any of these properties is called **semisimple**.

There are indeed modules that are not semisimple:

Example 101

Let $R = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \right\} \subseteq \mathrm{Mat}_2(F)$ acting on the module $M = \mathbb{F}^2$. Then the span N of $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ is a submodule that is not complemented.

Proof. If M is a sum of simple modules, that means that we can write $M = \sum_{j \in J} E_j$ for some (not necessarily finite) index set J, such that any element can be written as $x = \sum_j x_j$ with $x_j \in E_j$ and only finitely many x_j nonzero. We then have a direct sum if the representation of x is always unique, and the strategy for showing that (1) implies (2) is that we can discard some of the E_js and get a sum that is direct. But this is a Zorn's lemma argument – there is some subset $I \subseteq J$ such that $M = \sum_{j \in I} E_j$ is a direct sum, though we do not yet know that $\sum_{j \in I} E_j = M$. (Note that being direct also means that if $i \in I$, then $E_i \cap \sum_{j \in I, j \neq i} E_j = 0$.) We choose a maximal such subset I by Zorn's lemma, and we claim that $M = \sum_{j \in I} E_j$. It suffices to show that every E_j is contained in $\bigoplus_{i \in I} E_i$, since the E_js generate the

module M. Suppose otherwise for some E_j – then $E_j \cap \sum_{i\in I} E_i$ is a proper submodule of E_j, so by simplicity of E_j we must have $E_j \cap \sum_{i\in I} E_i = 0$. Thus $I \cup \{j\}$ would also yield a direct sum $M = \bigoplus_{i\in I+\{j\}} E_i$, contradicting maximality. (Here j is not in I because otherwise E_j would be contained in $\bigoplus_{i\in I} E_i$ in the first place.) So $\bigoplus_{i\in I} E_i$ must be a direct sum for M.

(2) implies (3) is very similar: if we can write $M = \bigoplus_{i\in J} E_i$ and we have a submodule $N \subset M$, then choose a subset $I \subset J$ maximal within the condition that $N \cap \sum_{i\in I} E_i = 0$ by Zorn's lemma. We can then show that $N \oplus \sum_{j\in I} E_j = M$ (otherwise we could add another j to I), and so we've found our P.

Finally, (3) implies (1) is the tricky part – it suffices to show that any nonzero submodule E of M contains a simple module. (Otherwise we can take the complement of the sum of all simple submodules of M, which we can do by complete reducibility, and arrive at a contradiction.) Let v be some nonzero element of E, and consider the submodule Rv. The map $a \mapsto av$ is a homomorphism $R \to Rv$, and we can let $\mathfrak{m}$ be a maximal ideal containing the kernel. The image $\mathfrak{m}v$ of $\mathfrak{m}$ is then a maximal submodule of Rv, so by complete reducibility we can let M' be an R-module such that $M = \mathfrak{m}v \oplus M'$. We claim that $Rv = \mathfrak{m}v \oplus (M' \cap Rv)$; it's clear if we put $+$ instead of $\oplus$, and to show we have a direct sum we can write $x \in Rv$ as $x = av + m'$ for $m' \in M'$ and then notice that $m' = x - av$ is in Rv because $x, av \in Rv$, and thus $m' \in M' \cap Rv$ and thus $M' \cap Rv \cong Rv/\mathfrak{m}v$ is simple because we've modded out by a maximal submodule. So we've exhibited a simple submodule of Rv, so in particular that is a simple submodule of E. □

18 February 22, 2023

We'll start by proving the last part of the dimension theorem today – recall that we wish to prove that for a local noetherian ring A with maximal ideal $\mathfrak{m}$, $d(A)$ (the degree of the Hilbert-Samuel polynomial), $\sigma(A)$ (the smallest number of generators of any $\mathfrak{m}$-primary ideal), and $\dim(A)$ (the Krull dimension) are equal. All that's left is to show that $\dim(A) \le d(A)$.

Proof. Suppose we have a chain of prime ideals $\wp_0 \subsetneq \wp_1 \subsetneq \cdots \subsetneq \wp_d = \mathfrak{m}$. We wish to show that d is at most the degree of the Hilbert-Samuel polynomial $\chi_{\mathfrak{m}}$ (which is the polynomial with $\chi_{\mathfrak{m}}(n) = \ell(a/\mathfrak{m}^n)$ for sufficiently large n). Notice that we can replace A by $A/\wp_0$, which does not change d but may decrease the values of $\chi_{\mathfrak{m}}$. Thus doing this cannot increase the degree of the polynomial (or else the values of the polynomial will eventually grow bigger), and thus we may assume without loss of generality that $\wp_0 = 0$ and that A is an integral domain.

We'll prove this by induction on d – the base case is a ring of dimension 0, but this is trivial. For the inductive step, let a be some nonzero element of $\wp_1$, let $\mathfrak{a} = (a)$, and let $\overline{A} = A/\mathfrak{a}$. Now $\overline{A}$ has a chain of ideals $\overline{\wp_1} \subsetneq \cdots \subsetneq \overline{\wp_d}$, with $\overline{\wp_i} = \wp_i/\mathfrak{a}$, and we know by induction that $d - 1 \le \deg \chi_{\overline{\mathfrak{m}}}$. It suffices now to show that $\deg \chi_{\mathfrak{m}} > \deg \chi_{\overline{\mathfrak{m}}}$. There is a homomorphism $A/\mathfrak{m}^n \to \overline{A}/\overline{\mathfrak{m}}^n$, whose kernel is $(\mathfrak{m}^n + \mathfrak{a})/\mathfrak{m}^n \cong \mathfrak{a}/(\mathfrak{a} \cap \mathfrak{m}^n)$. Thus the length can be written as $\ell(A/\mathfrak{m}^n) = \ell(\overline{A}/\overline{\mathfrak{m}}^n) + f(n)$, where $f(n) = \ell(\mathfrak{a}/\mathfrak{a} \cap \mathfrak{m}^n)$. We will prove that f is of the same degree and leading coefficient as $\chi_{\mathfrak{m}}$, so that subtracting will reduce the degree. f is indeed a polyomial for sufficiently large n, since it's the difference of two such terms which are polynomials for large enough n. But by the Artin-Rees lemma (from homework), we know that

$$\mathfrak{a} \cap \mathfrak{m}^n = \mathfrak{m}^{n-r}(\mathfrak{a} \cap \mathfrak{m}^r)$$

for some r depending only on $\mathfrak{a}$ and for all $n \ge r$. Then we have $\mathfrak{a}\mathfrak{m}^r \subseteq \mathfrak{a} \cap \mathfrak{m}^r \subseteq \mathfrak{a}$, and multiplying both sides by $\mathfrak{m}^{n-r}$ shows that $\mathfrak{a}\mathfrak{m}^n \subseteq (\mathfrak{a} \cap \mathfrak{m}^r)\mathfrak{m}^{n-r} \subseteq \mathfrak{a}\mathfrak{m}^{n-r}$, but the middle term is now $\mathfrak{a} \cap \mathfrak{m}^n$. So this means that (dividing the ideal $\mathfrak{a}$ by each of these terms)

$$\ell(\mathfrak{a}/\mathfrak{a}\mathfrak{m}^{n-r}) \le \ell(\mathfrak{a}/\mathfrak{a} \cap \mathfrak{m}^n) \le \ell(\mathfrak{a}/\mathfrak{a}\mathfrak{m}^n).$$

But now $\mathfrak{a}$ is principal, and A is an integral domain, so $\mathfrak{a}$ is isomorphic to A as an A-module. In other words, we also have

$$\ell(\mathfrak{a}/\mathfrak{m}^n\mathfrak{a}) = \ell(A/\mathfrak{m}^n) = \chi_{\mathfrak{m}}(n)$$

for large enough n, and thus the inequality is actually saying that

$$\chi_{\mathfrak{m}}(n-r) \leq f(n) \leq \chi_{\mathfrak{m}}(n)$$

for sufficiently large n. So that indeed means f must also be a polynomial of the same degree as χ_m and of the same leading order, yielding the result. □

(So the dimension theorem is a nice showcase of lots of techinques in commutative algebra. And the Artin-Rees lemma is also used to prove an important fact about $\mathfrak{a}$-adic topologies, which we are also seeing on our homework.)

We'll now return to **semisimplicity** again – last time, we proved that for a (not necessarily commutative) ring R, the following are equivalent for an R-module M: **(1)** M is a sum of simple R-modules (which are nonzero modules with no proper nonzero submodules), **(2)** M is a **direct** sum of simple R-modules, and **(3)** M is **completely reducible**, meaning that for any submodule N, we have some submodule P such that $M = N \oplus P$.

Definition 102

A ring R is **semisimple** if R is semisimple as a left R-module.

Lemma 103

If M is a semisimple R-module and N is a submodule of M, then N is semisimple.

Proof. By semisimplicity of M, N is complemented and thus we can write $M = N \oplus P$. Now for any submodule T of N, we have $M = T \oplus U$ for some R-module U. Since N is isomorphic to M/P (from the direct sum), we can define the image $\overline{U}$ of U in $\overline{M} = M/P$, and $\overline{M} \cong \overline{U} \oplus \overline{T}$. Then $\overline{T} = (T+P)/P \cong T$ because $T \cap P = 0$. Pulling back, since N is isomorphic to $\overline{M}$, we get a complement of T in N. Thus N is completely reducible, hence semisimple.

Alternatively, we can say that M is a (direct) sum of simple modules $M = \sum E_i$, and define the homomorphism $p : M \to N$ be the homomorphism $M \to M/P \cong N$. This is surjective, so N is the sum of the modules $p(E_i)$. Since E_i is simple, each $p(E_i)$ will either be zero or isomorphic to a simple module, and thus N is also a sum of simple modules. □

Lemma 104

If M is semisimple and $Q = M/K$ for some submodule K of M, then Q is semisimple.

Proof. By complete reducibility, $M \cong K \oplus P$ for some submodule P and Q is isomorphic to P, meaning that every quotient module is isomorphic to a submodule, hence semisimple. □

Lemma 105

An arbitrary direct sum $M = \bigoplus_{i \in I} M_i$ of semisimple modules is semisimple.

Proof. Each M_i is a direct sum of simple modules, and thus M is also such a sum. □

Proposition 106

If R is semisimple, then every R-module is semisimple.

Proof. If M is an R-module, then M is isomorphic to some free module $\bigoplus_{i\in I} R$ modulo an ideal, which is a quotient of a semisimple module, hence semisimple. □

Theorem 107 (Wedderburn)

A semisimple algebra over a field F must take the form $\bigoplus_{i=1}^{k} \mathrm{Mat}_{d_i}(D_i)$, where D_is are division algebras over F, and conversely such a ring is always semisimple.

(Remember that we're asking these rings to be semisimple over themselves.) In particular, if F is algebraically closed, then $D_i = F$, which is why doing representation theory over algebraically closed fields is nice. We may consult Lang for the proof – we won't go through it here. There's also the Jacobson density theorem, which we should take a look at on our own reference, and Burnside's theorem, which states that if $|G| = p^a q^b$ for primes p, q, then G is not a nonabelian simple group (which is easiest to prove using representation theory).

Next time, we'll prove Maschke's theorem, which states that whenever we have a field of characteristic zero or of characteristic p not dividing $|G|$, the group algebra $F[G]$ is semisimple. (A counterexample is done in the homework where F is a field of characteristic p and G is the cyclic group of order p.) Then we'll move on to the Schur orthogonality relations. The theme we'll see is that there are methods from group representation theory that have essential consequences in group theory but cannot be proved without the representation theory tools.

19 February 24, 2023

We've previously stated Maschke's theorem, which can be phrased in the following way: let G be a finite group, F a field, and $\mathrm{char}(F)$ either zero or a prime not dividing $|G|$. Then $F[G]$ is semisimple, meaning that every $F[G]$-module is completely reducible. Since representations $\pi : G \to \mathrm{GL}(V)$ (for some F-vector space V) correspond to $F[G]$-modules, and completely reducible modules are direct sums of simple modules, this implies that **representations can be written as direct sums of irreducible representations** – that is, if $\pi : G \to \mathrm{GL}(V)$ is a representation, then V is a direct sum of irreducible G-invariant subspaces (that is, there is no subspace that is also G-invariant, which is equivalent to being an $F[G]$-submodule).

Towards proving Maschke's theorem, let M be a module over R, and let N be a submodule. Consider the R-module homomorphisms $p : M \to M$ such that $p(M) = N$ and p acts as the identity on N. We call such an operator p a **projection operator**, and notice in particular that $p^2 = p$ (since applying p twice gets into N and then does nothing). In fact, being a projection operator is equivalent to the conditions that $N = p(M)$ and $p^2 = p$, and we can visualize this in the usual linear algebraic sense, and such a projection operator always yields a complement:

Lemma 108

Let $p : M \to M$ be a projection onto N. Then $M = N \oplus H$, where $H = \ker(M)$.

Proof. We may write any element of M as $m = n + h$, where $n = p(m)$ and $h = m - p(m)$. Then clearly we have $n \in N = \mathrm{Im}(p)$ and $h \in \ker(p)$, since $p(h) = p(m - p(m)) = p(m) - p^2(m) = p(m) - p(m) = 0$. Thus this is a valid decomposition for any m. Furthermore N and H only intersect trivially, since for any $x \in N \cap H$ we have $x = p(y)$ for

some y and thus $p(x) = p(p(y)) = p(y) = x$ but $p(x) = 0$ by being in the kernel. Thus we do have a direct sum, and N and H are both submodules because p is a homomorphism. □

So in the proof of Maschke's theorem, we will **construct** such a projection operator:

Proof of Maschke's theorem. We must prove that any submodule N of an $F[G]$-module M is complemented as an $F[G]$-module. It is indeed complemented as an F-vector space, so we can write $M = N \oplus H$, where H is a vector subspace of M. We then have a vector space projection $p' : M \to N$ with kernel H (that is, write m uniquely in the direct sum $n + h$ and take $p'(m) = n$), but the problem is that this may not be a module homomorphism. Instead, the trick is to modify p' by **averaging** and define

$$p(x) = \frac{1}{|G|} \sum_{g \in G} g p'(g^{-1} x)$$

(here is where we use the hypothesis that the characteristic is not a prime dividing $|G|$, so that $\frac{1}{|G|}$ is invertible). We wish to show that p is an $F[G]$-module homomorphism and that p is actually a projection onto N. (Applying Lemma 108 would then allow us to take $H = \ker(p)$ and we'd be done.)

First we check that $p(x) \in N$ and that if $x \in N$, then $p(x) = x$. The first part is true because $p'(g^{-1}x)$ is in N for each g, and N is a G-invariant subspace so $gp'(g^{-1}x)$ is in N for each g; taking the average of these values then again gives us something in N. And the second part is true because if $x \in N$, then $g^{-1}(x) \in N$ as well, so $gp'(g^{-1}x) = g(g^{-1}x) = x$ for all $g \in G$ (since p' is a projection onto N). Averaging this over all g again gives us x. Thus p is a projection onto N.

Finally, this map is actually a G-module homomorphism – it suffices to check that $\gamma p(x) = p(\gamma x)$ for any $\gamma \in F[G]$, and by linearity we can just check this when $\gamma \in G$. We have

$$p(\gamma x) = \frac{1}{|G|} \sum_{g} g p'(g^{-1}\gamma x) = \frac{1}{|G|} \sum \gamma g p'(g^{-1}\gamma^{-1}\gamma x) = \gamma \left(\frac{1}{|G|} \sum g p'(g^{-1}(x)) \right)$$

where in the middle equality we've made a substitution $g \mapsto \gamma g$, and the right-hand side is indeed $\gamma p(x)$. So we've turned the projection into a G-module homomorphism, and thus the proof is complete. □

Proposition 109

Let R be a semisimple ring. Then R has a finite number of isomorphism classes of simple modules – in particular, this means that over a field of characteristic zero, any finite group G has a finite number of equivalence classes of irreducible representations (by applying this to $R = F[G]$).

(This last part is true even if we were working in characteristic p, but we'll make use of semisimplicity so our proof wouldn't work.)

Proof. Since R is semisimple, it is a direct sum of simple submodules – in other words, we can write $R = \bigoplus_{i \in J} L_i$ for some simple left ideals L_i. A priori, J could be infinite, but we can write $1 = \sum_{i \in J} \ell_i$ for ℓ_i zero for all but finitely many i. Thus we can write $1 = \sum_{i \in I} \ell_i$ for a **finite** index set I.

Lemma 110

If L is a simple left ideal and M is a simple module, then either $LM = 0$ or $M \cong L$ as R-modules.

Proof of lemma. Suppose $LM \neq 0$. Then pick some $m \in M$ such that $Lm \neq 0$, and consider the module homomorphism $\phi : L \to M$ which sends x to xm. We have $\phi(rx) = r\phi(x)$, so ϕ is a nonzero module homomorphism, and we claim ϕ is an isomorphism. Indeed, the kernel of ϕ is a proper submodule of L, hence must be zero because L is simple, and then the image of ϕ is a nonzero submodule of M, hence must be M itself. Thus we've shown that $M \cong L$ since ϕ is both injective and surjective.

(Part of this argument is Schur's lemma, which we'll discuss in more detail after this proof.) □

So returning to $1 = \bigoplus_{i \in I} \ell_i$, we can show that every irreducible module is isomorphic to one of the L_is where $i \in I$. Indeed, $1 \cdot M = M$, meaning that $\ell_i M \neq 0$ for some $i \in I$, and then we can apply the lemma to show that $M \cong L_i$. □

Proposition 111 (Schur's lemma)
If M and N are simple modules over R, then either $\mathrm{Hom}_R(M, N) = 0$ or $M \cong N$. Furthermore, if they are isomorphic we may assume $M = N$, and every nonzero element of $\mathrm{End}_R(M)$ is invertible.

Proof. This is the same as before: suppose $\phi : M \to N$ is any element of $\mathrm{Hom}_R(M, N)$ with $\phi \neq 0$. Then $\ker \phi$ is a proper submodule of M, hence must be zero, and the image of ϕ is a nonzero submodule of N, hence must be all of N, and we've constructed an isomorphism. In particular, every nonzero element is invertible by taking the inverse of this isomorphism, which is also a module homomorphism. □

Definition 112
Let $\pi : G \to \mathrm{GL}(V)$ be a representation. The **character** of π, denoted χ_V or χ_π, is defined via $\chi_\pi(g) = \mathrm{tr}(\pi(g))$.

Example 113
For any homomorphism $\theta : G \to \mathbb{C}^\times$, we can define a corresponding one-dimensional representation $\pi_\theta : G \to \mathrm{GL}(\mathbb{C})$ where $\pi_\theta(g) = \theta(g)\mathrm{Id}_{\mathbb{C}}$. So θ is its own character, since one-dimensional matrices can be thought of as just numbers. Thus we will call a homomorphism $\theta : G \to \mathbb{C}^\times$ a **linear character** (and this is terminology often used in group theory).

Going forward, **we'll mostly assume that** $F = \mathbb{C}$ (mostly we just need characteristic zero, and later on we will want algebraically closed). Looking ahead to next class, we may define an inner product on the set of functions on G, given by

$$\langle f_1, f_2 \rangle = \frac{1}{|G|} \sum_{g \in G} f_1(g)\overline{f_2(g)}.$$

This gives us a finite-dimensional Hilbert space structure, and the big result (which we'll prove next time) is that if χ_1, χ_2 are characters of irreducible modules M_1, M_2, then $\langle \chi_1, \chi_2 \rangle = 1$ if $M_1 \cong M_2$ and 0 otherwise. So in particular by Schur's lemma this is the dimension of $\mathrm{Hom}_G(M_1, M_2)$ – then by bilinearity this relation between the inner product and dimension will hold for general modules.

20 February 27, 2023

Today, we'll discuss permutation representations, the regular representation, and a bit about characters in preparation for Schur orthogonality. All representations will be over the base field $\mathbb{C}$ today.

First, let G be a finite group acting on a set X (meaning we have a map $G \times X \to X$ sending $(g, x) \to g \cdot x$ such that $(g_1 g_2)x = g_1(g_2 x)$). If we then let $\mathcal{F}_X$ be the free $\mathbb{C}$-vector space on X, then we have a representation $\pi : G \to \mathrm{GL}(\mathcal{F}_X)$ in which we just extend the group action by linearity.

$$\pi(g)\left(\sum_{x \in X} a_x \cdot x\right) = \sum a_x (gx).$$

This is called the **permutation representation**.

Proposition 114

The character of the the permutation representation is

$$\chi_X(g) = \text{number of fixed points of } x \mapsto gx.$$

Indeed, we just choose the elements of X as a basis of $\mathcal{F}_X$, and then all entries of the matrix will be 1 or 0 (with a 1 in the (x, y) entry if $gy = x$). Then we have 1s on the diagonals corresponding to fixed points.

Example 115

Let $G = S_4$ act on the set $\{1, 2, 3, 4\}$. Then if g is the element $(143)(2)$ in cycle notation, then $\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$ is the corresponding matrix, with a trace of 1 because of the sole fixed point 2.

This permutation representation is usually not irreducible, since $\mathcal{F}_X$ has an invariant vector $\xi = \sum_{x \in X} x$. Then $g\xi = \xi$ for all g, so $\mathbb{C}\xi$ is a one-dimensional copy of the **trivial representation** (which sends everything to the identity). So now by complete reducibility (using Maschke's theorem), $\mathcal{F}_X$ splits as

$$\mathcal{F}_X = \mathbb{C}\xi \oplus \mathcal{F}_x^0,$$

where $\mathcal{F}_X^0$ is a complementary subspace to ξ. In fact we don't really need Maschke's theorem to see this – the subspace should be

$$\mathcal{F}X^0 = \left\{\sum a_x x : \sum a_x = 0\right\}.$$

Since the character of the trivial representation is just identically 1, the character χ is the number of fixed points minus 1.. It turns out this representation being irreducible is equivalent to the group action being doubly transitive, but we won't go into detail for that just yet.

Example 116

If $G = S_3$ acts on $\{1, 2, 3\}$, then there are three conjugacy classes, namely $\mathrm{id}, (123)$, and (12). We then have $\chi_X^0(\mathrm{id}) = 2, \chi_X^0((123)) = -1, \chi_X^0((12) = 0$, and it turns out this is an irreducible representation (we'll see why later).

Definition 117

There is always one permutation representation that we can exhibit for any finite group G, in which we have G act on itself by left multiplication (so sending (g, x) to gx for any $g \in G$, $x \in G$, where gx is the ordinary group multiplication). The corresponding permutation representation (where we do **not** remove the one-dimensional trivial representation) is then called the **regular representation**.

Then $\mathcal{F}_G$ can be identified with $\mathbb{C}[G]$ – both of them are the free vector space over the group G. And the computation of the character ρ for this representation is easy – a fixed point $gx = x$ occurs only if $g = \text{id}$, and thus id has $|G|$ fixed points and everything else has no fixed points, meaning $\rho(\text{id}) = |G|$ and $\rho = 0$ otherwise.

Proposition 118

For any representation $\pi : G \to \text{GL}(V)$ with corresponding character χ, we have $\chi(g^{-1}) = \overline{\chi(g)}$ (this is complex conjugation; in particular, this is why we are using $\mathbb{C}$ as the base field)

Proof. Since g is a member of a finite group, we know that $g^N = 1$ for some N. Thus $\pi(g)^N = 1$, meaning that all eigenvalues are Nth roots of unity with absolute value 1. The fact that $\pi(g)^N = 1$ also implies that $\pi(g)$ is diagonalizable, so we can choose a basis of eigenvectors for g $(v_1, \cdots, v_d)$ with $\pi(g)v_i = \varepsilon_i v_i$. Then $\pi(g)^{-1}v_i = \varepsilon_i^{-1}v_i$, but for roots of unity $\varepsilon_i^{-1} = \bar{\varepsilon}_i$. Since the trace is the sum of the eigenvalues, the desired relation holds for $\chi(g^{-1})$ and $\chi(g)$. □

In a previous homework assignment, we considered the following situation:

Proposition 119

Let V_1, V_2 be vector spaces and $T_1 : V_1 \to V_1$ and $T_2 : V_2 \to V_2$ be two linear transformations. If we then let $\Omega = \text{Hom}_{\mathbb{C}}(V_1, V_2)$, we can define a map $\tau : \Omega \to \Omega$ via $\tau(\phi) = T_2 \circ \phi \circ T_1$. Then $\text{tr}(\tau) = \text{tr}(T_1)\text{tr}(T_2)$.

Proof. Say that T_1, T_2 have bases $x_1, \cdots, x_n$ and $y_1, \cdots, y_m$ respectively, so that $T_1 x_i = \sum_j a_{ij} x_j$ and $T_2 x_k = \sum_\ell b_{k\ell} y_\ell$. With respect to these bases, we can identify $\text{Hom}(V_1, V_2)$ with $\text{Mat}_{n\times m}(\mathbb{C})$, with the basis of elementary matrices $E_{i,\ell}$ (where $E_{i,\ell}(x_j) = x_\ell$ if $i = j$ and 0 otherwise). Then we can also identify endomorphisms of T_1 as $\text{End}(V_1) \cong \text{Mat}_n(\mathbb{C})$ and $\text{End}(V_2) \cong \text{Mat}_m(\mathbb{C})$, so that τ maps ϕ to $B\phi A$. Then for any elementary matrix, thought of as a basis element, we have

$$\tau(E_{i\ell}) = \sum_{j,k} a_{ij} b_{k,\ell} E_{jk},$$

meaning that $\text{tr}(\tau)$ is the sum of the diagonal entries $\sum_{i=j,k=\ell} a_{ij} b_{k\ell} = \sum_i a_{ii} \sum_k b_{kk} = \text{tr}(A)\text{tr}(B) = \text{tr}(T_1)\text{tr}(T_2)$, as desired. □

Also note the following fact:

Proposition 120

Let Ω be a complex vector space and $\pi : G \to \text{GL}(\Omega)$ be a (not necessarily irreducible) representation. Letting Ω^G be the group of invariants – that is, the set of $x \in \Omega$ fixed by all $\pi(g)$ – we have

$$\dim \Omega^G = \frac{1}{|G|} \sum_{g \in G} \chi(g).$$

Proof. Define the map $p : \Omega \to \Omega$ via $p = \frac{1}{|G|}\sum_{g\in G}\pi(g)$. Then p is a projection with image Ω^G, since

$$\pi(g)p(v) = \frac{1}{|G|}\pi(g)\sum_{h\in G}\pi(h)v = \frac{1}{|G|}\sum_{h\in V}\pi(h)v = p(v)$$

by relabeling the order of the elements, and since $p(v) = \frac{1}{|G|}\sum v = v$ for any $v \in \Omega^G$. (So this is very similar to the proof of Maschke's theorem.) Thus p is idempotent, and Ω splits as $\Omega^G \oplus (\ker p)$. With respect to a basis whose first $\dim \Omega^G$ elements are exactly the elements of Ω^G, and the rest are in $\ker(p)$, p has matrix $\begin{bmatrix} I_{\Omega^G} & 0 \\ 0 & 0 \end{bmatrix}$ in block form, and the trace of this matrix is just the dimension of Ω^G. But by definition of p, the trace of p will be exactly $\frac{1}{|G|}\sum_{g\in G}\operatorname{tr}(\pi(g))$, which is the right-hand side. □

We will now apply the logic above to a pair of representations.

Theorem 121 (Schur orthogonality)
Let π_1, π_2 be two representations with corresponding G-modules V_1, V_2 and characters χ_1, χ_2. Then the dimension of $\operatorname{Hom}_G(V_1, V_2)$ (G-module morphisms, not just linear transformations) is $\frac{1}{|G|}\sum_{g\in G}\chi_1(g)\overline{\chi_2(g)}$. (This is an inner product which we will denote $\langle\chi_1, \chi_2\rangle$.) In particular (by Schur's lemma) if V_1, V_2 are irreducible, then the inner product is 1 if $V_1 \cong V_2$ and 0 otherwise.

Proof. Let $\Omega = \operatorname{Hom}_{\mathbb{C}}(V_1, V_2)$ be the space of **vector space** transformations, and define the representation $\Pi : G \to \operatorname{End}(\Omega)$ via

$$\Pi(g)\phi = \pi_2(g)\phi\pi_1(g)^{-1}.$$

We claim ϕ is a G-module homomorphism $V_1 \to V_2$ if and only if $\phi \in \Omega^G$ for Π. Indeed, being a G-module homomorphism means that $\phi\pi_1(g) = \pi_2(g)\phi$ (applying ϕ can be done before or after applying π), and rearranging that exactly yields $\Pi(g)\phi = \phi$. Now we know that the dimension of $\operatorname{Hom}_G(V_1, V_2)$ is the dimension of Ω^G, which is $\frac{1}{|G|}\sum\chi_\Pi(g)$. But now $\chi_\Pi(g)$ is the trace of $\phi \mapsto \pi_2(g)\phi\pi_1(g)^{-1}$, which is $\chi_2(g)\chi_1(g^{-1}) = \chi_2(g)\overline{\chi_1(g)}$; plugging in yields the result. □

We'll see some applications of this fact next time!

21 March 1, 2023

Last time, we showed that for any finite group G, there are finitely many irreducible representations (or equivalently, finitely many distinct isomorphism classes of $\mathbb{C}[G]$-modules). We can let these representations be $V_1, \cdots, V_k$ (corresponding to maps $\pi_i : G \to \operatorname{GL}(V_i)$). We proved last time that for any two characters χ, θ of representations $\pi : G \to \operatorname{GL}(V)$ and $\sigma : G \to \operatorname{GL}(W)$, we have

$$\langle\chi, \theta\rangle = \frac{1}{|G|}\sum_g \chi(g)\overline{\theta(g)} = \dim \operatorname{Hom}_{\mathbb{C}[G]}(V, W).$$

So combining with Schur's lemma and applying this to our irreducible representations, we find that

$$\langle\chi_i, \chi_j\rangle = \delta_{ij}.$$

Noticing that the character of a representation is called a **class function**, meaning that it is constant on conjugacy classes (since the matrix $\pi(gxg^{-1})$ is conjugate to $\pi(x)$, the traces $\chi(gxg^{-1})$ and $\chi(x)$ are the same). We can thus

define the function space $L^2(G)$ to be the set of functions on G with the inner product $\langle f_1, f_2\rangle = \frac{1}{|G|}\sum_{x\in G} f_1(x)\overline{f_2(x)}$, and then we have the subspace $L^2(G)_{\text{class}}$ (which is the subset of $L^2(G)$ which is constant on each conjugacy class). It will turn out that $\chi_i \in L^2(G)_{\text{class}}$ are not just orthonormal but also a basis of $L^2(G)_{\text{class}}$, and since $\dim L^2(G)_{\text{class}}$ is the number of conjugacy classes of G this means the number of irreducible representations is equal to the number of conjugacy classes. (And in fact, we can go from this to getting an orthonormal basis on all of $L^2(G)$.)

Last time, we also showed that if G acts on a set X, then the action extends to a representation of G on the free vector space $\mathcal{F}_X$ and yields a character χ_X in which $\chi_X(g)$ is the number of fixed points of g. (And we can construct the "reduced permutation character" χ_X^0 by removing the invariant subspace spanned by $\sum_{x\in X} x$, which is often useful too.) When G is acting on itself by left multiplication, we then get the **(left) regular representation** (which has character $\rho(g) = |G|$ for $g = \text{id}$ and 0 otherwise).

Theorem 122

If χ_i are the characters of the irreducible representations, then the decomposition of the regular representation is given by $\rho = \sum d_i\chi_i$.

In other words, the multiplicity of a representation V_i is just its degree d_i.

Proof. By Maschke's theorem, we know that $\mathbb{C}[G]$ is isomorphic to some direct sum of the V_is, yielding $\rho = \sum n_i\chi_i$ for some integers n_i. Then we can use the orthogonality relations to find that

$$n_i = \langle \rho, \chi_i\rangle = \frac{1}{|G|}\sum \rho(g)\overline{\chi_i(g)} = \frac{1}{|G|}\cdot|G|\cdot\overline{\chi_i(\text{id})},$$

since ρ is zero for everything except $g = \text{id}$. But $\chi_i(\text{id})$ is the trace of the identity matrix, which is exactly the dimension d_i of the representation V_i. □

Remark 123. *We could go deeper into what's going on behind the scenes here, but we'll just talk about it briefly – we stated Wedderburn's theorem earlier without proof, and as a corollary of that (because $\mathbb{C}[G]$ is a semisimple algebra over an algebraically closed field) $\mathbb{C}[G]$ is a finite direct sum of matrix rings $\text{Mat}_{d_i}(\mathbb{C})$. Each such matrix ring is a two-sided ideal with a unique simple module $\mathbb{C}^{d_i}$. We then get a representation of G by injecting $G \to \mathbb{C}[G]$ and then restricting to $\text{Mat}_{d_i}(\mathbb{C})$, which acts on $\mathbb{C}^{d_i}$. And this is where the irreducible representation theorems come from – decomposing the matrix ring into copies of the simple module, we get that $\text{Mat}_{d_i}(\mathbb{C})$ is a direct sum of d_i copies of $\mathbb{C}^{d_i}$, denoted $L_1 \oplus \cdots \oplus L_{d_i}$, where we could make L_i the set of matrices only nonzero in the ith column. So the module of the regular representation, $\mathbb{C}[G]$, will indeed be a direct sum of d_i copies of V_i, summed over all irreducible representations V_i. And such an interpretation also allows us to deduce Schur orthogonality.*

We may think of group representation theory as a nonabelian version of Fourier analysis, and in the coming lectures we'll prove two results of that type (though there are many others) which don't require representation theory in their statements but for which it is the right language for the proofs.

Theorem 124 (Burnside's p^aq^b theorem)

Any group of order p^aq^b, where p, q are (distinct) primes, is solvable. Thus, any nonabelian simple group has $|G|$ divisible by at least three primes.

(Here note that p-groups are nilpotent because they have a normal subgroup of index p, so we do have a chain of normal subgroups.) This result was proved without representation theory methods in the 1960s by Thompson and Bender, but the original proof remains easier. And this is in fact one of the big steps towards the classification of finite simple groups.

Theorem 125

Suppose G is a permutation group which acts on X transitively, and assume that only the identity element of G has more than one fixed point (this is called a **Frobenius group**). Then the set $\{g \in G : g = \text{id or } g \text{ has no fixed points}\}$ is a normal subgroup of G.

This result has actually never been proved without representation theory methods.

Example 126

An example of a Frobenius group is $G = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : a \in \mathbb{F}_q^\times, b \in \mathbb{F}_q \right\}$ acting on $\mathbb{F}_q$ via $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : x \mapsto ax + b$. Then the normal subgroup in question is the set of translations.

Both of those proofs will come later in the class, and for now we'll turn to the topic of **computing all irreducible representations and values of their characters**. It turns out that there is a computer program called Gap (included in Sage) that can do this, and there is an atlas of finite simple groups which we can find online as well. The idea is to let $\mathcal{C}_1, \cdots, \mathcal{C}_k$ be the conjugacy classes of G and to choose a representation g_i of each $\mathcal{C}_i$. For example, for S_3, we can start a table as follows:

	1	2	3
	id	(123)	(12)
χ_1			
χ_2			
χ_3			

Here the numbers 1, 2, 3 indicate the number of elements in each conjugacy class, and a representative of each conjugacy class is written below them. Now there are two linear (one-dimensional) representations, namely the trivial one (which acts as the identity matrix on every element and thus has $\chi(g) = 1$ for all g) and the sign permutation $S_n \to \{\pm 1\}$ which sends even permutations to 1 and odd permutations to -1. The point here is that any homomorphism $\chi : G \to \mathbb{C}^\times$ is the character of a one-dimensional representation $\pi_\chi : G \to \mathrm{GL}(\mathbb{C})$ sending v to $\chi(g)v$, with trace again equal to χ. So we can fill in the first two rows of the character table as follows:

	1	2	3
	id	(123)	(12)
$\chi_1 = \chi_{\text{triv}}$	1	1	1
$\chi_2 = \chi_{\text{sign}}$	1	1	-1
χ_3			

We're now wanting to fill in the third row to find the last irreducible representation. Recall that we have the reduced permutation representation for any S_n, where S_n acts on $\{1, 2, \cdots, n\}$ with $\chi_\chi^0(g)$ equal to one less than the number of fixed points of g. Thus we claim that this is the last entry in our table:

	1	2	3
	id	(123)	(12)
$\chi_1 = \chi_{\text{triv}}$	1	1	1
$\chi_2 = \chi_{\text{sign}}$	1	1	-1
$\chi_3 = \chi^0_{\{1,2,3\}}$	2	-1	0

To see this, we can prove the following lemma:

Lemma 127

If χ is any character with $\langle \chi, \chi \rangle = 1$, then χ is irreducible.

In particular, we have $\langle \chi_3, \chi_3 \rangle = \frac{1}{6}(\chi(\mathrm{id})^2 + 2\chi((123))^2 + 3\chi((12))^2)$ (since we have to take the multiplicity of each conjugacy class into account), which is $\frac{1}{6}(4 + 2 \cdot 1 + 3 \cdot 0) = 1$. So we have indeed found all of the irreducible representations of S_3.

Proof. Suppose χ is a character of (π, V). Writing V as a sum of copies of irreducible representations, such that $\chi = \sum n_i \chi_i$ for nonnegative integers n_i, we get

$$\langle \chi, \chi \rangle = \sum n_i n_j \langle \chi_i, \chi_j \rangle = \sum n_i^2.$$

If this is equal to 1, then all but one of the n_is is zero and the remaining one is 1, so χ is indeed just a single copy of some irreducible representations. □

We'll do another computation next time and talk a bit more about linear characters, and we'll also prove that indeed the number of irreducible representations is indeed exactly equal to the number of conjugacy classes.

22 March 3, 2023

Today's lecture will go over a few more basics of representation theory, so that we can discuss induced representations, Mackey theory, and the Frobenius theorem next week. We've previously shown that the irreducible characters satisfy $\langle \chi_1, \chi_2 \rangle = 1$ if $\pi_1 \cong \pi_2$ and 0 otherwise (by thinking about the dimension of the Hom-space $\mathrm{Hom}_G(\pi_1, \pi_2)$ where G acts on $\mathrm{Hom}_{\mathbb{C}}$ via $g\phi = \pi_2 \phi \pi_1^{-1}$ and using a formula from homework where we computed the dimension of the G-fixed-points, and by using Schur's lemma), so we have an orthonormal set. We also showed, by Schur orthogonality relations, that the regular representation is a direct sum of $d_i = \dim(V_i)$ copies of the corresponding irreducible representations V_i, and in fact the simple modules of $\mathbb{C}[G]$ can be identified with irreducible representations via Wedderburn's theorem.

The reason we go through all of this alternate reasoning is that we now want to show that the set of characters of irreducible representations is actually a basis of $L^2(G)_{\text{class}}$, the set of functions on G constant on each conjugacy class:

Theorem 128

The number of irreducible representations of G is equal to the number of conjugacy classes of G.

We'll do a proof here following the textbook:

Proof. We can compute the dimension of the center $Z(\mathbb{C}[G])$ in two ways: first of all, $\xi = \sum_{g \in G} a_g \cdot g$ is in the center if and only if a_g is constant on conjugacy classes (since conjugating will permute the a_gs within a class). So letting the conjugacy classes be $\mathcal{C}_1, \cdots, \mathcal{C}_k$, we get a basis via the functions $\kappa_i = \sum_{x \in \mathcal{C}_i} x$, and thus the dimension is k. On the other hand, we can compute by writing (by Wedderburn's theorem) $\mathbb{C}[G] \cong \bigoplus_{i=1}^{\text{number of irreducibles}} \mathrm{Mat}_{d_i}(\mathbb{C})$, and the center is one-dimensional for each summand and spanned by I_{d_i}. So the dimension must also be the number of irreducible representations. □

We'll now turn to the mechanics of computing character tables: the first step is to find the linear (one-dimensional) representations. Then after that, we can often find the d_is because we know how many there are (the number of

conjugacy classes), we know how many are 1s (from the previous step), and we know $\sum d_i^2 = |G|$, which limits the number of total possibilities. Sometimes there will be tricks for producing some irreducible characters, and in fact induced representations allow us to produce all of them as long as we know the characters of subgroups of G.

But we'll start from the beginning here – let G' be the **derived group** or **commutator subgroup**, which is the subgroup generated by all elements of the form $xyx^{-1}y^{-1}$. Notice that any homomorphism $G \to A$ for an abelian group A contains G' in its kernel (since $xyx^{-1}y^{-1}$ will always be sent to the identity in A, as everything commutes there). So any one-dimensional representation $\chi : G \to \mathbb{C}^\times$ factors through the abelianization G/G'.

Now notice that if G and H are two groups with representations (π, V) and (σ, W) representations of G, H respectively, then we have a representation $\pi \otimes \sigma : G \times H \to \mathrm{GL}(V \otimes W)$, which has character $\chi_{V\otimes W} : (g,h) \mapsto \chi_V(g)\chi_W(h)$. Furthermore, $V \otimes W$ will be irreducible if V and W are irreducible – this holds because

$$\langle \chi_{V\otimes W}, \chi_{V\otimes W}\rangle = \frac{1}{|G|}\frac{1}{|H|}\sum_{g\in G\times H} |\chi_V(g)|^2|\chi_W(g)|^2$$

has the sum factor into $|G||H|$, so this inner product is indeed 1. And in fact the number of conjugacy classes of $G \times H$ is the product of the number of conjugacy classes of G and of H, and the $\chi_{V\otimes W}$s are all orthogonal, so that gives us all irreducible representations of $G \times H$. So now because G/G' is a finite abelian group, it is a product of cyclic groups, and we know the characters of a cyclic group $\langle \sigma : \sigma^n = 1\rangle$ are of the form $\chi_a(\sigma^m) = e^{2\pi i am/n}$, where $a \in \{0, 1, \cdots, n-1\}$. So that tells us that the one-dimensional irreducible representations of G are bijection with the irreducible representations of G/G'.

Example 129

Consider the dihedral group $D_4 = \langle x, y : x^4 = y^2 = 1, yxy^{-1} = x^{-1}\rangle$ of order 8. The conjugacy classes of this group are $\{1\}, \{x, x^{-1}\}, \{x^2\}, \{y, x^2y\}, \{xy, x^{-1}y\}$.

Thus we will have five irreducible representations, and one will always be the trivial character. Furthermore, the commutator subgroup $G' = Z(D_4)$ is generated by x^2. Indeed, $\langle x^2\rangle$ is normal, and $|G/Z(G)| = 4$ so $G/Z(G)$ is an abelian group, meaning $G' \subseteq Z(G)$ (here we use that for $N \triangleleft G$, we have G/N abelian if and only if G' is contained in N). Furthermore $xyx^{-1}y^{-1} = x^2$, so $\langle x^2\rangle$ is contained in G' as well.

So G/G' is generated by the cosets $\overline{x}, \overline{y}$ satisfying the relations $\overline{x}^2 = \overline{y}^2 = (\overline{xy})^2 = 1$. So this group is isomorphic to the Klein four group $\mathbb{Z}_2 \times \mathbb{Z}_2$, whose characters on $1, \overline{x}, \overline{y}, \overline{xy}$ are either $(1,1,1,1)$, $(1,1,-1,-1)$, $(1,-1,1,-1)$ or $(1,-1,-1,1)$. So pulling all of these back to the dihedral group lets us fill in most of the table:

	1	2	1	2	2
	1	x	x^2	y	xy
χ_1	1	1	1	1	1
χ_2	1	1	1	−1	−1
χ_3	1	−1	1	1	−1
χ_4	1	−1	1	−1	1
χ_5					

There is then one more representation to find: we know that $8 = |D_4| = d_1^2 + d_2^2 + d_3^2 + d_4^2 + d_5^2$, so $d_5 = 2$. And now there are different ways to proceed: one is to note that the regular representation satisfies $\chi_1 + \chi_2 + \chi_3 + \chi_4 + 2\chi_5 = \chi_{\text{reg}}$, where χ_{reg} is 8 on the identity and 0 everywhere else. That yields the following table:

	1	2	1	2	2
	1	x	x^2	y	xy
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	-1	1	1	-1
χ_4	1	-1	1	-1	1
χ_5	2	0	-2	0	0

Alternatively, we can make use of the fact that D_4 acts on the vertices of a square via rotation (x) and reflection (y), and thus we can take the reduced permutation character $\chi^0_\square$ to get a representation of degree 3 which takes values $3, -1, -1, -1, 1$ on the correpsonding cnojugacy classes. And now we can calculate its inner product with each of $\chi_1, \chi_2, \chi_3, \chi_4$, and we will see that $\langle \chi^0_\square, \chi_4 \rangle = 1$. We thus have $\chi^0_\square = \chi_4 + \chi$ for some other representation χ of degree 2, and then when we compute $\langle \chi, \chi \rangle$ we get 1 and thus this is the last irreducible representation.

23 March 6, 2023

We'll discuss induced representations, Frobenius groups, and Mackey theory this week. The idea is that for any subgroup $H \subseteq G$ of a group, we get a functor sending representations of G to representations of H via restriction, and we wish to show that this has an adjoint functor (actually both a left and right adjoint) sending representations of H to representations of G. This has a close relationship with character theory – a representation (π, V) of H with character χ leads us to a representation (π^G, V^G) with character χ^G characterized as follows. For any G-module W, we have

$$\mathrm{Hom}_G(W, V^G) \cong \mathrm{Hom}_H(W, V)$$

(so this is the "right adjoint" relation – the isomorphism commutes with homomorphisms $VV \to V'$ and we can form a commutative square, but we won't care about that too much in this class), and here all we're saying is that the dimensions of the two vector spaces are the same. Indeed, if θ is the character of W, then the isomorphism above can be formulated as $\boxed{\langle \theta, \chi^G \rangle_G = \langle \theta, \chi \rangle_H}$, and this is equivalent (if we don't care about the naturality) from the inner product formula saying that $\langle \psi, \chi \rangle$ is the dimension of the corresponding Hom space between G-modules. We'll first prove that we indeed do have this equality:

Proof of the character form. Suppose $\psi_1, \cdots, \psi_k$ are the irreducible characters of G. Then any class function (function on G constant on conjugacy classes) is a linear combination $\theta = \sum d_i \psi_i$, and θ is a character if and only if the d_is are all nonnegative integers. So now if we have a character χ of H, we can produce such a character of G by setting $d_i = \langle \chi, \psi_i \rangle_H$ (which are nonnegative integers, since both χ and ψ_i restricted to H are representations and thus can be written as linear combinations of irreducible representations in H), then letting χ^G be $\sum d_i \psi_i$. We then have to prove the boxed relation, which is called **Frobenius reciprocity**. By linearity, we can just check this for $\theta = \psi_i$ for some arbitrary i, but then this holds because $\langle \chi, \psi_i \rangle_H = d_i = \langle \chi^G, \psi_i \rangle_G$ – first equality by definition and second equality by orthogonality of the ψ_is. □

We can also sketch an alternate strategy, which generalizes to Lie groups and gives us a bit more to work with.

Alternate proof sketch. We will work with modules – let (π, V) be a representation of H with character χ. We define

$$V^G = \{\text{space of functions } f : G \to V | f(hg) = \pi(h) f(g) \quad \forall h \in H\}$$

(that is, we ask for a property under left translation), and now define the action $\pi^G : G \to \text{End}(V)$ via right translation, meaning that $(\pi^G(g)f)(x) = f(xg)$. By associativity of the group action this endomorphism does indeed produce another element of V^G, and we need to check that $\text{Hom}_G(W, V^G) \cong \text{Hom}_H(W, V)$. We will only sketch this part: to define the forward map, take an element $\Phi \in \text{Hom}_G(W, V^G)$ and map it to $\phi \in \text{Hom}_H(W, V)$ via

$$\phi(w) = \Phi(w)(\text{id}_G)$$

(since $\Phi(W)$ is a function $G \to V$). We may check that ϕ is an H-module homomorphism, since

$$\phi(hw) = \Phi(hw)(\text{id}_G) = \pi^G(h)\Phi(w)(\text{id}_G) = \Phi(w)(h) = \pi(h)\Phi(w)(\text{id}_G) = \pi(h)\phi(w)$$

where we use the definition of π^G and then the property of invariance under right translation for the two blue equalities. And then we just need to check that $\Phi \mapsto \phi$ is actually an isomorphism of vector spaces. □

Remark 130. *It turns out more generally we can also require that f has compact support on G/H, which is "compact induction." Then we get a left adjoint in one case and a right adjoint in the other, but these two ideas coincide for finite groups, which is the case we're considering here.*

Theorem 131

Let χ be a character of H and extend χ to a function $\dot{\chi}$ on G which is equal to χ on H and zero otherwise. Then the induced character χ^G is obtained via the formula

$$\chi^G(x) = \frac{1}{|H|} \sum_{g \in G} \dot{\chi}(g^{-1}xg).$$

(If H were normal, then the averaging process still only keeps the nonzero part within H. So the induced character from a **normal** subgroup actually still has support inside H.)

Proof. The right-hand side is a class function because we've averaged over all conjugates, and thus it is sufficient to show that if $\tau(x) = \frac{1}{|H|}\dot{\chi}(g^{-1}xg)$, then $\langle \tau, \theta \rangle_G = \langle \tau, \theta \rangle_H$ for any character θ of G (since χ_G is the **only** class function satisfying this inner product relation). We have

$$\langle \tau, \theta \rangle_G = \frac{1}{|G|} \sum_{x \in G} \tau(x)\overline{\theta(x)} = \frac{1}{|G|} \cdot \frac{1}{|H|} \sum_{x \in g} \sum_{g \in G} \dot{\chi}(g^{-1}xg)\overline{\theta(x)}.$$

Swapping the order of summation and reparameterizing $x \mapsto gxg^{-1}$, this simplifies to

$$= \frac{1}{|G|} \cdot \frac{1}{|H|} \sum_{g \in g} \sum_{x \in G} \dot{\chi}(x)\overline{\theta(gxg^{-1})}.$$

But since θ is a class function, this is also equal to

$$= \frac{1}{|G|} \cdot \frac{1}{|H|} \sum_{g \in g} \sum_{x \in G} \dot{\chi}(x)\overline{\theta(x)},$$

and now the nonzero contribution comes only from $x \in H$ and the sum doesn't depend on the value of g, so this is just $\frac{1}{|H|} \sum_{x \in H} \dot{\chi}(x)\overline{\theta(x)} = \langle \chi, \theta \rangle_H$, as desired. □

This formula can be rewritten – $\dot{\chi}$ is invariant under conjugation by H, so we in fact have $\dot{\chi}(h^{-1}xh) = \dot{\chi}(x)$ for any $h \in H$. So χ^G is constant on cosets gH, and if we choose a set of left coset representatives $g_1, \cdots, g_n$ so that

$G = \bigcup g_i H$, then

$$\chi^G(x) = \sum_i \dot{\chi}(g_i^{-1} x g_i) = \sum_{G/H} \dot{\chi}(g^{-1} x g)$$

(the last equality is just notation for choosing one representative from each coset).

Induced representations are sometimes irreducible (but sometimes not, even if χ is irreducible), and there is in fact a criterion coming from Mackey theory that tells us when it will be. We'll do that later on, and for now we'll just do some examples:

Example 132

Consider the group G of order 21 generated as $\langle x, y : x^7 = y^3 = 1, yxy^{-1} = x^2 \rangle$. We can construct most of the character table below, where ω is a third root of unity:

	1	3	3	7	7
	1	x	x^{-1}	y	y^2
χ_1	1	1	1	1	1
χ_2	1	1	1	ω	ω^2
χ_3	1	1	1	ω^2	ω
χ_4	3	?	?	?	?
χ_5	3	?	?	?	?

Recall that we compute this character table by first noting that $G' = \langle xrangle$ is a normal 7-Sylow subgroup, and since $G/G' \cong \mathbb{Z}/3\mathbb{Z}$ is abelian we have $G' \subset \langle x \rangle$, while since $yxy^{-1}x^{-1} = x$ we have $\langle x \rangle \subset G'$. Then the first three characters are linear characters coming from $\mathbb{Z}_3$, and then χ_4 and χ_5's degrees are computed by noting that $d_4^2 + d_5^2 = 18$ can only occur if we have a three-dimensional representation. But because inducing $H \to G$ multiplies the degree by $[G : H]$ (that is, $\chi^G(1) = [G : H]\chi(1)$), we may try to realize χ_4 and χ_5 as induced representations from linear characters if we can find a subgroup of index 3. Indeed, the coset representations for G/G' are $1, y, y^2$, and we can consider the character $\chi : H \to \mathbb{C}^*$ sending $\chi(x^k) = \zeta^k$, where ζ is a seventh root of unity. We then have

$$\chi_4 = \chi^G(x) = \dot{\chi}(x) + \dot{\chi}(yxy^{-1}) + \dot{\chi}(y^2xy^{-2}).$$

Since H is a normal subgroup of G, this will be supported only within G', and we have $\chi_4(x) = \zeta + \zeta^2 + \zeta^4$ and $\chi_4(x^{-1}) = \zeta^{-1} + \zeta^{-2} + \zeta^{-4}$. Taking the conjugate then gives us χ_5 as well.

We cannot always obtain all representations by inducing in this way, but there is a theorem of Brauer that for any character χ of G there are **elementary subgroups** (that is, a product of a cyclic group and a p-group) $E_1, \cdots, E_m$, linear characters $\psi_1, \cdots, \psi_m$, and integers $d_1, \cdots, d_m$, such that $\chi = \sum d_i \psi_i^G$. So we just need to supplement this process with an additional step of taking linear combinations.

24 March 8, 2023

We'll discuss **Frobenius groups** today, which we introduced a few lectures ago but only briefly:

Definition 133

A **Frobenius group** is a group G along with a faithful group action of G on X which is transitive, such that no group element other than the identity fixes more than one point.

Example 134

Suppose $X = \mathbb{F}_q$ is a finite field, and G is the set of transformations $a \mapsto ax + b$, which is isomorphic to the matrix group of elements of the form $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$. Then $|G| = q(q-1)$, and only the identity element fixes two points (since the values of two points determine the line $x \mapsto ax + b$).

Notice in particular that G has two notable subgroups. The first is the **isotropy subgroup**

$$H = \{g \in G : gx_0 = x_0\}$$

for some fixed base point x_0 – for example, if $x_0 = 0$ then we get the subgroup $x \mapsto ax$ (with $b = 0$), and this always works for any permutation representation. But there is also a **normal** subgroup in our case, which is the set of translations $x \mapsto x + b$ (with $a = 1$), and this is called the **Frobenius kernel**.

Theorem 135 (Frobenius)

Let G (acting on some set X) be a Frobenius group. Then the set $\{\mathrm{id}_G\} \cup \{g \in G \text{ with no fixed points}\}$ is a normal subgroup of G.

As we've mentioned previously, this result has always required representation theory to prove. The hard part here is proving that this is actually a subgroup – once we do that it'll be normal, since the subgroups $H_x = \{g \in G : gx = x\}$ (sometimes called the **Frobenius complements**) are all conjugate because the action is transitive, and if $\gamma x = y$ then $\gamma H_y \gamma^{-1} = H_x$.

Fix $x_0 = X$ and $H = H_{x_0}$ (with the definition above), and let

$$K = \{\mathrm{id}_G\} \cup \left(G - \bigcup_{\gamma \in G} \gamma H \gamma^{-1} \right).$$

Then being in this set and not the identity means we have no fixed points. So if $\gamma \notin H$, then $\gamma H \gamma^{-1} \cap H = \mathrm{id}_G$ (since $\gamma x_0 \neq x_0$, and $\gamma H \gamma^{-1} = H_{\gamma x_0}$, and $H_{\gamma x_0} \cap H_{x_0} = 1$ by definition of a Frobenius group).

Proposition 136

Let G be a group, H a nontrivial subgroup of G, and assume that if $x \in G$, then either $x \in H$ or $xHx^{-1} \cap H = \{\mathrm{id}_G\}$. Then G is a Frobenius group.

Proof. We want to construct a group action – let $X = G/H$ be the set of cosets gH of G. Then the stabilizer of xH is xHx^{-1}, so by our hypothesis no element fixes both $1 \cdot H$ and $x \cdot H$; it's easy to go from this to seeing that no element has two fixed points. □

Before we prove Frobenius's theorem, we can extrapolate and deduce some implications. Then the set of elements $K = \{\mathrm{id}_G\} \cup \bigcup_{x \in G} xHx^{-1}$ satisfies $HK = G$ and $H \cap K = \mathrm{id}_G$, so G is in fact a semidirect product. We then get maps $H \to G \to G/K$, given by inclusion and then projection, such that the composite map is an isomorphism. So in particular, if (π, V) is a representation of H (in fact this works for general homomorphisms as well), we can extend it to a representation of G in the following way: use the isomorphism to get a representation on G/K, and then pull it back to G. This way of representation is always valid because the composite map $G \to G/K \cong H$ is the identity map, so it will agree with π. So the strategy for Frobenius's theorem will in fact be to prove this fact, showing that a representation can be extended.

Lemma 137

Let G be a Frobenius group acting on X, x_0 some element of X, and $H = H_{x_0}$. Then any representation of H can be extended to a representation of G.

Proof. Induction is part of the bag of tricks here – we know that if χ is a character of H, then we can write $\chi = \sum d_i \psi_i$, where ψ_i are the irreducible characters of H and d_i are nonnegative integers. We can relax this condition and say that a class function χ on H is a **generalized character** if $\chi = \sum d_i \psi_i$, now allowing d_i to be **any** integers (so in particular it is the difference of two ordinary characters). For any such character χ of H, we know from last lecture that $\chi^G(g) = \frac{1}{|H|} \sum \dot{\chi}(xgx^{-1})$, with the Frobenius reciprocity relation $\langle \chi^G, \psi \rangle = \langle \chi, \psi \rangle_H$ for any ψ; this relation continues to hold for generalized characters by linearity.

So this allows us to also induce generalized characters in the same way as ordinary characters as follows. Define $d = \chi(\mathrm{id}_G)$, so that $\chi = \chi_0 + d \cdot 1_H$ (where 1_H is the trivial character sending everything to 1). Then $\chi_0(\mathrm{id}_G) = 0$, χ_0 is a generalized character, and then we can define $\hat{\chi} = \chi_0^G + d \cdot 1_G$ (getting the induced representation and then adding back d copies of the trivial character). We must show that $\hat{\chi}$ agrees with χ on H; indeed for $x = 1$ both sides are equal to d (and this is why we had to subtract off $d1_H$ in the first place), since we can recall that the formula for the induced representation is

$$\hat{\chi}_0^G(x) = \frac{1}{|H|} \sum_{g \in G} \dot{\chi}_0(gxg^{-1})$$

so if $x = \mathrm{id}_G$ then all terms on the right are 0. Now if we suppose $x \in H$ is not the identity. We know that for any $g \notin H$, we have $H \cap gHg^{-1} = \mathrm{id}_G$, so in fact

$$\hat{\chi}_0^G(x) = \frac{1}{|H|} \sum_{g \in G} \dot{\chi}_0(gxg^{-1}) = \frac{1}{|H|} \sum_{g \in H} \dot{\chi}_0(gxg^{-1}) = \chi_0(x).$$

Thus $\chi_0 = \hat{\chi}_0^G$, and adding d to both sides yields $\hat{\chi} = \chi$ for all non-identity $x \in H$.

To finish the proof, we must now show that $\langle \hat{\chi}, \hat{\psi} \rangle_G = \langle \chi, \psi \rangle_H$ for any generalized character χ of H. (In other words, the mapping is an isometry under the inner product.) We may write $\chi = \chi_0 + d \cdot 1_H$ and $\psi = \psi_0 + c \cdot 1_H$ (where $d = \chi(\mathrm{id}_G)$ and $c = \psi(\mathrm{id}_G)$). By linearity, it suffices to handle the two cases where $\chi_0 = 0$ and where $d = 0$ separately, and the same two cases for ψ. In the case where $\chi_0, \psi_0 = 0$, we have $\chi = d, \psi = c$ everywhere, which leads to $\hat{\chi} = d, \hat{\psi}$ everywhere, and thus both sides are just dc. Otherwise, we may assume without loss of generality that $\chi = \chi_0$ (and $d = 0$). Then because $\chi(\mathrm{id}_G) = 0$, we have by Frobenius reciprocity that

$$\langle \hat{\chi}, \hat{\psi} \rangle_G = \langle \chi, \hat{\psi} \rangle_H = \langle \chi, \psi \rangle_H$$

(the last part because $\hat{\psi}$ agrees with ψ on H), which proves the result. (The key point here is that $\hat{\chi}$ is not the induced representation of χ, so we need to get rid of the $d \cdot 1_H$ part.) □

Corollary 138

Any character χ of H can be extended to a character of G.

Proof. Without loss of generality, we may assume that χ is irreducible, so that $\hat{\chi}$ satisfies $\langle \hat{\chi}, \hat{\chi} \rangle = 1$. Write $\hat{\chi} = \sum d_i \theta_i$ as a sum of irreducible representations of G; then $\sum d_i^2 = 1$ so in fact $\hat{\chi}$ is either an irreducible representation of G or its negative. Then $\chi(1) = \hat{\chi}(1) > 0$, so we rule out the latter possibility. □

The result of Frobenius' theorem now follows immediately:

Proof of Theorem 135. Take a faithful representation of H, such as the regular representation, and extend it to a representation of G. Its kernel K is a normal subgroup, and it is easy to see that K is in fact $\{1\} \cup \{G - \bigcup xHx^{-1}\}$. □

25 March 10, 2023

Mackey theory is a powerful method which makes use of double cosets to get information about induced representations. For example, if G is a finite group, H is a subgroup, and π is a representation of H, we may want to know when the induced representation $\pi^G = \mathrm{Ind}_H^G(\pi)$ is irreducible (so we can produce irreducible representations). Or we may be interested in seeing what representations occur if we induce a representation from H_1 and then restrict to some subgroup H_2.

Example 139

Let π be a representation of S_n and let $\lambda = (\lambda_1, \cdots, \lambda_k)$ be a partition of n. (For example, the partitions of 5 are $(5), (4,1), (3,2), (3,1,1), (2,2,1)$, and $(1,1,1,1,1)$.) Then we can consider the Young subgroup $S_\lambda = S_{\lambda_1} \times \cdots \times S_{\lambda_k}$ (that is, permuting only among the first λ_1 elements, the next λ_2, and so on).

One result that Mackey theory is then able to tell us (along with some combinatorics) is that if we start from the trivial representation on S_λ and induce a representation on S_n, and we start from the sign representation on S_μ and also induce a representation on S_n, then $\mathrm{Hom}(\mathrm{Ind}_{S_\lambda}^{S_n}(1), \mathrm{Ind}_{S_\mu}^{S_n}(\mathrm{sgn}))$ is one-dimensional if λ, μ are **conjugate partitions** (meaning that we draw the **Young diagrams** for the two partitions and they are reflections of each other over the diagonal, for example $(3,2)$ and $(2,2,1)$). In particular, this means that the image of this Hom space is an irreducible representation of S_n, and thus all irreducible representations are constructed this way.

More generally, we want to know how to compute $\mathrm{Hom}(\pi_{H_1}^G, \pi_{H_2}^G)$ for representations π_1, π_2 of subgroups H_1, H_2 of G. Let χ_1, χ_2 be the corresponding characters – the dimension of the Hom space is then $\langle \chi_1^G, \chi_2^G \rangle_G$, and we will need to talk about double cosets to answer this question.

Definition 140

A **double coset** of G is a subset of the form $H_2 \gamma H_1$, where H_1, H_2 are subgroups of G.

For fixed H_1, H_2, any two double cosets are either equal or disjoint, meaning that we may write $G = \bigcup_{i=1}^k H_2 \gamma_i H_1$ for double coset representatives γ_i. (Alternatively, we can use the notation $G = \bigcup_{\gamma \in H_2 \backslash G / H_1} H_2 \gamma H_1$, where again we sum over one representative γ per equivalence class.) Now for any $\gamma \in G$ we may define

$$H_\gamma = H_2 \cap \gamma H_1 \gamma^{-1},$$

which is a subgroup of H_2 and also conjugate to a subgroup of H_1 (since $\gamma^{-1} H_\gamma \gamma \subseteq H$). So H_γ can be thought of as a subgroup of both H_1 and H_2 (just with an extra conjugation in the former case).

Lemma 141

Let $\gamma_1, \cdots, \gamma_k$ be a set of double coset representatives for G, so that $G = \bigcup H_2 \gamma_i H_1$. For each $\gamma = \gamma_i$, let $\delta_{i1}, \delta_{i2}, \cdot$ be a set of coset representatives for H_2 / H_{γ_i}. Then we have that $G = \bigcup \delta_{ij} \gamma_i H_1$ as a disjoint union.

In other words, we've obtained a set of coset representatives for G/H_1: we can alternatively write

$$G = \bigcup_{\gamma \in H_2 \backslash G / H_1} \bigcup_{\delta \in H_2 / H_\gamma} \delta \gamma H_1.$$

Proof. Every element of G can be written as $h_2\gamma h_1$ for some $h_1 \in H_1$, $h_2 \in H_2$, and $\gamma \in H_2 \setminus G/H_1$. We want to ask when $h_2\gamma h_1 = h_2'\gamma' h_1$; we must have $\gamma = \gamma'$, but we have some flexibility for h_2, since $h_2\gamma H_1 = h_2'\gamma H_1$ implies that $h_2^{-1}h_2'\gamma H_1 = \gamma H_1$ and thus $\gamma^{-1}h_2^{-1}h_2'\gamma \in H_1 \implies h_2^{-1}h_2' \in \gamma H_1 \gamma^{-1}$. Since $h_2, h_2' \in H_2$, that means $h_2^{-1}h_2' \in H_\gamma$. So h_2, h_2" produce the same coset $h_2\gamma H_1$ if and only if h_2, h_2' are in the same coset of H_2/H_γ. (And this reasoning is all reversible.) □

Theorem 142 (Mackey theory, version 1)

We have

$$\langle \chi_1^G, \chi_2^G \rangle_G = \sum_{\gamma \in H_2 \backslash G/H_1} \langle {}^\gamma\chi_1, \chi_2 \rangle_{H_\gamma},$$

where ${}^\gamma\chi_1$ corresponds to a representation π_1^γ and is the character given by

$${}^\gamma\chi_1(x) = \chi_1(\gamma^{-1}x\gamma).$$

Proof. By Frobenius reciprocity, we know that $\langle \chi_1^G, \chi_2^G \rangle_G = \langle \chi_1^G, \chi_2 \rangle_{H_2}$. By the formula for the induced representation, we know that $\chi_1^G(x) = \sum_{G/H_1} \dot{\chi}_1(\gamma^{-1}x\gamma)$, so the left-hand side of the theorem statement is (plugging into Frobenius reciprocity)

$$\frac{1}{|H_2|}\sum_{x\in H_2} \chi_1^G(x)\overline{\chi_2(x)} = \frac{1}{|H_2|}\sum_{x\in H_2}\sum_{\tau \in G/H_1} \dot{\chi}_1(\tau^{-1}x\tau)\overline{\chi_2(x)}.$$

If we now split into double coset representatives, this becomes

$$= \frac{1}{|H_2|}\sum_{x\in H_2}\sum_{\gamma\in H_2\backslash G/H_1}\sum_{\delta \in H_2/H_\gamma} \dot{\chi}_1(\gamma^{-1}\delta^{-1}\delta\gamma)\overline{\chi_2}(x).$$

But now if we swap the order of sums, the inner sum becomes a sum over x and x is mapped to $\delta x\delta^{-1}$, and $\chi_2(\delta x\delta^{-1}) = \chi_2(x)$ because χ_2 is a class function. So we get rid of dependence on one of the variables δ, and we're just left with

$$= \frac{1}{|H_2|}\sum_{\gamma\in H_2\backslash G/H_1} [H_2 : H_\gamma] \sum_{x\in H_2} \dot{\chi}_1(\gamma^{-1}x\gamma)\overline{\chi_2(x)}.$$

But now this sum is zero unless $\gamma^{-1}x\gamma$ is in H_1, so in fact $x \in H_2 \cap \gamma H_1\gamma^{-1} = H_\gamma$. So now we can remove the dot on χ_1, and we're left with

$$= \sum_{\gamma\in H_2\backslash G/H_1} \frac{1}{|H_\gamma|}\sum_{x\in H_\gamma} \chi_1(\gamma^{-1}x\gamma)\overline{\chi_2(x)},$$

which is exactly the expression on the right that we were looking for. □

In the special case where $H_1 = H_2$ is a normal subgroup N of G, we can prove directly that

$$\chi_1^G(x) = \sum_{\gamma\in G/N} {}^\gamma\chi(x)$$

for any $x \in N$, and that $\chi_1^G(x) = 0$ if $x \notin N$. (Note that if N is normal, then $N\backslash G/N = N$.) This doesn't require Mackey theory to prove:

Proposition 143

If N is a normal subgroup of G, then G/N acts on representations of N by conjugation. Let χ be an irreducible character of N. Then χ^G is irreducible if and only if χ is not fixed by any non-identity coset $\omega \in G/N$.

In particular, ${}^{\gamma}\chi(g) = \chi(\gamma^{-1}g\gamma)$ only depends on the coset γN, since χ is a class function. So to prove this result, by Frobenius reciprocity we have

$$\langle \chi^G, \chi^G \rangle_G = \langle \chi^G, \chi \rangle_N = \left\langle \sum_{\gamma \in G/N} \chi^{\gamma}, \chi \right\rangle,$$

which is the number of $\gamma \in G/N$ such that ${}^{\gamma}\chi = \chi$. So if χ is not fixed by any nontrivial coset, then this calculation shows that $\langle \chi^G, \chi^G \rangle = 1$.

We'll do some more examples next time!

26 March 13, 2023

Last time, we started discussing Mackey theory – one version of this takes two subgroups H_1, H_2 of G with representations (π_1, V_1) and (π_2, V_2) of those subgroups. We can then consider the homomorphisms $\mathrm{Hom}_G(V_1^G, V_2^G)$, and we showed using characters that we can compute

$$\dim \mathrm{Hom}_G(V_1^G, V_2^G) = \langle \chi_1^G, \chi_2^G \rangle = \sum_{\gamma \in H_2 \backslash G / H_1} \langle {}^{\gamma}\chi_1, \chi_2 \rangle_{H_\gamma},$$

where $H_\gamma = H_2 \cap \gamma H_1 \gamma^{-1}$ and where the "twisted" character ${}^{\gamma}\chi_1$ is given by ${}^{\gamma}\chi_1(x) = \chi_1(\gamma^{-1}x\gamma)$. (So here we are summing over a set of double coset representatives R, such that $G = \bigsqcup_{\gamma \in R} H_2 \gamma H_1$. In particular, we can change γ by an element of H_1 on the right or by an element of H_2 on the left, and the construction of ${}^{\gamma}\chi_1$ and H_γ does depend on the choice of representative up to H_2 but we will end up getting the same values of inner products because we end up in a conjugate subgroup.)

We've done a few examples in lecture where the subgroups have been normal, making the computations easier, but in our homework we saw a more interesting case:

Example 144

Let $G = \mathrm{GL}(2, F)$ for some finite field $F = \mathbb{F}_q$. Then $|G| = (q^2 - 1)(q^2 - q)$, and we may let B be the Borel subgroup of upper-triangular matrices with nonzero (invertible) entries on the diagonal. We then have $|B| = (q-1)^2 q$ and $[G : B] = q + 1$. So now if χ_1, χ_2 are two linear characters of $F^\times$, we can define the linear character $\chi : B \to \mathbb{C}^*$ via

$$\chi\left(\begin{bmatrix} y_1 & x \\ 0 & y_2 \end{bmatrix}\right) = \chi_1(y_1)\chi_2(y_2).$$

We can then induce χ from B to G, and it turns out that if χ_1, χ_2 are distinct then the induced representation $\mathrm{Ind}_B^G(\chi)$ is irreducible. (This turns out to compute about half of the irreducible representatives for $\mathrm{GL}(2, F)$.

This was on our homework, but we'll discuss it in some more detail here. We'll compute more generally by letting ψ_1, ψ_2 be two other linear characters of $\mathbb{F}^\times$ and similarly define $\psi : B \to \mathbb{C}^*$ in the same way as χ. We then want to compute $\langle \chi^G, \psi^G \rangle$. The double cosets of G are given by the **Bruhat decomposition**

$$G = B \cdot I \cdot B \cup B \cdot \omega \cdot B, \quad \omega = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

(The same argument works for $\mathrm{GL}(n, F)$, just with $n!$ double cosets corresponding to the $n!$ elements of the symmetric group.) Then $B_\gamma = B \cap \gamma B \gamma^{-1}$, where γ is chosen to be either the identity matrix or ω, so B_γ is either B itself (for I) or the diagonal subgroup (for ω). So to compute using Mackey theory we need to compute two terms $\langle \chi, \psi \rangle_B + \langle {}^{\omega}\chi, \psi_T \rangle$.

Since these are one-dimensional representations, each term will be 1 if the two characters agree and 0 otherwise – the former is only 1 if $\chi_1 = \psi_1, \chi_2 = \psi_2$, and the latter is only 1 if $\chi_1 = \psi_2, \chi_2 = \psi_1$. So if $\chi_1 \neq \chi_2$ but $\psi = \chi$ we have $\langle \psi, \psi \rangle_G = 1$ and thus χ is irreducible. On the other hand, if $\chi_1 \neq \chi_2$ then χ is isomorphic to the corresponding representation where we swap χ_1, χ_2.

All of this also extends (with nuances) to irreducible **infinite-dimensional** representations of $\mathrm{GL}(2, F)$ for any nonarchimedean local field. (We can search up "principal series representations" for more, and this is relevant to automorphic forms.)

There is actually another theorem of Mackey theory which we can use for other computations, which involves computing the induced representation of some representative (π, V) of H_1 and then restricting to another subgroup of H_2:

Theorem 145 (Mackey theory, version 2)
Take $H_\gamma = H_2 \cap \gamma H_1 \gamma^{-1}$ as before. Then we have

$$\mathrm{Ind}_{H_1}^G(V)|_{H_2} \cong \bigoplus_{\gamma \in H_2 \backslash G / H_1} \mathrm{Ind}_{H_\gamma}^{H_2}({}^\gamma\pi),$$

where ${}^\gamma\pi$ is defined via ${}^\gamma\pi(h) = \pi(\gamma^{-1} h \gamma)$ (where in particular $\gamma^{-1} h \gamma \in H_1$ so this makes sense).

The idea is that the sum over double cosets is like embedding H_1 into G in different ways. So instead if inducing and then restricting, we can restrict to H_γ and then induce, but we must take a direct sum over different possibilities.

Proof. We'll show that we have equality of characters

$$\chi^G|_{H_2} = \sum_{\gamma \in H_2 \backslash G / H_1} = \mathrm{Ind}_{H_\gamma}^{H_2}({}^\gamma\chi),$$

and to do this we can take the inner product with an arbitrary character ψ of H_2. We have by Frobenius reciprocity that

$$\langle \chi^G|_{H_2}, \psi \rangle_{H_2} = \langle \chi^G, \psi^G \rangle_G,$$

and now by version 1 of Mackey theory this simplifies to

$$= \sum_{\gamma \in H_2 \backslash G / H_1} \langle {}^\gamma\chi, \psi \rangle_{H_\gamma},$$

but by Frobenius reciprocity again this simplifies to $\sum_\gamma \langle {}^\gamma\chi^G, \psi \rangle_G$, which is indeed the character of the right-hand side. Thus the two representatives are indeed isomorphic. □

We'll do one more example using the earlier form of Mackey theory to show some interesting computations:

Example 146
Let $G = S_5$, $H_1 = S_3 \times S_2$, and $H_2 = S_2 \times S_2 \times S_1$ (so H_1 only permutes among the first three and last two elements separately, and similarly for H_2). We claim that

$$\mathrm{Hom}_{S^5}\left(\mathrm{Ind}_{H_1}^G(1), \mathrm{Ind}_{H_2}^G(\mathrm{sgn})\right)$$

is one-dimensional.

We must find a set of double coset representatives for $H_2\backslash G/H_1$, and we will do so by thinking of permutations as matrices. For example, $h_1 = (123)(45)$ corresponds to $\begin{bmatrix} 0 & 0 & 1 & & & \\ 1 & 0 & 0 & & & \\ 0 & 1 & 0 & & & \\ & & & 0 & 1 \\ & & & 1 & 0 \end{bmatrix}$, with zeros also in the remaining entries. If we now think of γ as being in blocks labeled by $\begin{bmatrix} 1 & 1 & 1 & 2 & 2 \\ 1 & 1 & 1 & 2 & 2 \\ 3 & 3 & 3 & 4 & 4 \\ 3 & 3 & 3 & 4 & 4 \\ 5 & 5 & 5 & 6 & 6 \end{bmatrix}$ (where 1 through 6 label groups, not matrix entries), we see that we can permute entries in those six blocks using $S_3 \times S_2$ on the right (using column operations) and $S_2 \times S_2 \times S_1$ on the left (using row operations). So the idea is that we can rearrange columns and rows within blocks, but the blocks themselves must stay the same. In other words, each block has entries of 0 and 1, and the rank g_i of block i must stay constant.

Additionally, we also see that $g_1 + g_2 = 2$ (because we must have one nonzero entry per row of the big matrix), and similarly $g_3 + g_4 = 2, g_5 + g_6 = 1$. By the same reasoning on columns, $g_1 + g_3 + g_5 = 3, g_2 + g_4 + g_6 = 2$. And we can check that those are the only possible constraints using some combinatorics. So we can now basically compute all possibilities: we have

$$\begin{bmatrix} g_1 & g_2 \\ g_3 & g_4 \\ g_5 & g_6 \end{bmatrix} \in \left\{ \begin{bmatrix} 2 & 0 \\ 0 & 2 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 2 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 2 \\ 2 & 0 \\ 1 & 0 \end{bmatrix} \right\},$$

where for example the first can correspond to the coset representative $\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$, which represents the permutation (354). But now we claim we will have $\langle {}^{\gamma}1, \mathrm{sgn} \rangle_{H_\gamma} = 0$ as long as H_γ contains a transposition. Indeed, ${}^{\gamma}\chi_1 = 1$ on H_γ is orthogonal to $(\chi_2)_{H_\gamma} = \mathrm{sgn}$, and we will check that only the blue one has no transpositions. Thus the Hom space is indeed one-dimensional. And the corresponding generalization (working exactly the same way) is that for any partitions λ, μ of n, we can compute $\mathrm{Hom}(\mathrm{Ind}_{S_\lambda}^{S_n}(1), \mathrm{Ind}_{S_\mu}^{S_n}(\mathrm{sgn}))$ (the idea is that the matrix of g_is must only contain 0s and 1s); in particular if λ is the conjugate partition of μ, this will always be one-dimensional with irreducible image. In other words, **partitions characterize irreducible representations of** S_n.

27 March 15, 2023

Our first topic for today is to prove that the degree of an irreducible representation of G divides the order of the group $|G|$. First, recall a fact that we have proved on our homework, which is that for any character χ of an irreducible representation (π, V), then for any $g \in G$ in some conjugacy class $\mathcal{C}$, we have $\frac{|\mathcal{C}|\chi(g)}{\chi(1)}$ an algebraic integer. Indeed, this can be proved by considering the center of $\mathbb{Z}[G]$, which has a basis of elements of the form $K_i = \sum_{g \in \mathcal{C}_i} g$ (one for each conjugacy class). Then we get a representation of $\mathbb{C}[G]$ by extending π by linearity; since K_i is in the center of $\mathbb{C}[G]$, it acts as a scalar by Schur's lemma (since it commutes with the action of G). We then have $\pi(K_i) = \omega_\pi(K_i)\mathrm{Id}_V$ for

some $\omega_\pi(K_i) \in \mathbb{C}$.

Each $\omega_\pi(K_i)$ is an algebraic integer, since we have $K_iK_j = \sum_k a_{ijk}K_k$ for some coefficients $a_{ijk} \in \mathbb{Z}$ and thus we also have $\omega_\pi(K_i)\omega_\pi(K_j) = \sum a_{ijk}\omega_\pi(K_k)$. That means the K_is generate a ring which is finitely generated over $\mathbb{Z}$, so by our usual criterion those elements must be algebraic integers. Remembering that having a faithful $\mathbb{Z}[\alpha]$-module finitely generated as a $\mathbb{Z}$-module proves that α is integral, we see that $M = \mathbb{Z}[\omega_\pi(K_i)]$ is finitely generated, so each $\omega_\pi K_i$ is an algebraic integer. But

$$\omega_\pi(K_i) = \sum_{g \in \mathcal{C}_i} \pi(g_i) = \omega_\pi(k_i)\mathrm{Id}_V,$$

and taking traces on both sides yields $|\mathcal{C}_i|\chi(g) = \omega_\pi(K_i)\chi(1)$, which yields the result that we want.

So now we can use this:

Proposition 147

For any irreducible representation of G with character χ, we have $\chi(1)||G|$.

Proof. We have

$$1 = \langle \chi, \chi \rangle \implies |G| = \sum_{g \in G} \chi(g)\overline{\chi(g)} = \sum_{i=1}^{k} |\mathcal{C}_i|\chi(g)\overline{\chi(g)},$$

where we have broken up the sum into conjugacy classes. But this means that

$$\frac{|G|}{\chi(1)} = \sum_{i=1}^{k} \frac{|\mathcal{C}_i|\chi(g)}{\chi(1)} \cdot \overline{\chi(g_i)}.$$

Now the left-hand side is rational, and the right-hand side is an algebraic integer (since $\overline{\chi(g_i)}$ is a sum of roots of unity, each of which is an algebraic integer, and the other term we've also proved is an algebraic integer). Since the only rational numbers that are algebraic integers are integers, this proves the claim. □

In general, for an irreducible character χ of g corresponding to a representation (π, V), we can define

$$Z(\chi) = \{g \in G : \pi(g) \text{ is a scalar endomorphism of } V\}.$$

The idea is that we can recognize whether $g \in Z(\chi)$ just by looking at the character table:

Proposition 148

With the notation above, we have $g \in Z(\chi)$ if and only if $|\chi(g)| = \chi(1)$.

Proof. Since $\pi(g)$ is diagonalizable, the matrix is similar to a diagonal matrix with entries $(\varepsilon_1, \cdots, \varepsilon_d)$ with all $|\varepsilon_i| = 1$. Then the triangle inequality says that $|\sum \alpha_i| = \sum |\alpha_i|$ if and only if the α_i are all proportional over $\mathbb{R}^+$, which can only occur if they are all equal because they are of unit length. □

Also, notice that $Z(\chi)$ is a normal subgroup (since conjugating $g \in Z(\chi)$ corresponds to conjugating a scalar matrix, which just recovers the original scalar matrix again) – this can be useful in various situations.

Theorem 149

Let $\mathcal{C}$ be a conjugacy class of G and χ be an irreducible character, and suppose that $\chi(1)$ and $|\mathcal{C}|$ are coprime. Then either $g \in Z(\chi)$ or $\chi(g) = 0$.

(This result is particularly useful if we know that G is a simple group.)

Proof. By Bezout's lemma, we can find $a, b \in \mathbb{Z}$ such that $a\chi(1) + b|\mathcal{C}| = 1$. Multiplying this by $\frac{\chi(g)}{\chi(1)}$, we see that

$$a\chi(g) + b\frac{|\mathcal{C}\chi(g)}{\chi(1)} = \frac{\chi(g)}{\chi(1)}.$$

Now both terms on the left-hand side are algebraic integers, so $\frac{\chi(g)}{\chi(1)}$ is also an algebraic integer. In particular, it is an algebraic integer of a particular type: the eigenvalues of $\pi(g)$ are roots of unity $\varepsilon_1, \cdots, \varepsilon_d$, so $\frac{\chi(g)}{\chi(1)} = \frac{\varepsilon_1+\cdots+\varepsilon_d}{d}$. Any Galois conjugate of this is also of this form for some other roots of unity $\varepsilon_1', \cdots, \varepsilon_d'$, meaning all Galois conjugates have absolute value at most 1. Thus the norm of $\frac{\chi(g)}{\chi(1)}$ in $\mathbb{Q}(\chi(g))$ over $\mathbb{Q}$ has absolute value at most 1, and the norm must lie in $\mathbb{Z}$. So if the norm has absolute value 1, then $|\chi(g)| = \chi(1)$ and thus (by Proposition 148) it is in $Z(\chi)$; otherwise the norm is 0 and thus $\chi(g) = 0$. □

Theorem 150

Let G be a **nonabelian** simple group. Then the only way for a conjugacy class to have order a power of p is if $\mathcal{C} = \{\mathrm{id}_G\}$.

(Both this result and the previous one are likely due to Burnside.) In particular, this means that the non-identity conjugacy classes of a simple group each have order divisible by at least two primes – indeed, for $G = A_5$, there are conjugacy classes of size 1 (from the identity), 20 (from 3-cycles), 15 (from pairs of transpositions), and two of size 12 (from (12345) and (13524)).

Proof. Consider the regular representation of G, which has d_i copies of each irreducible representation χ. In particular, this means that

$$\sum_{\chi} \chi(1)\chi(g) = \begin{cases} |G| & g = \mathrm{id}_G, \\ 0 & \text{otherwise.} \end{cases}$$

Suppose the conjugacy class $\mathcal{C}_g$ containing g has order a power of p. If χ is not the trivial representation, then $Z(\chi)$ is trivial (because it is a normal subgroup that is not all of G, since π is faithful and G is nonabelian). By Theorem 149, this means that either $\chi(1)$ is divisible by p or $\chi(g) = 0$ (since in the latter case $\chi(1)$ and $|\mathcal{C}_g|$ are relatively prime). So now for any fixed $g \neq \mathrm{id}_G$, we can take the equation from above and write it as

$$0 = 1 + \sum_{\chi \text{ nontrivial}} \chi(g)\chi(1).$$

But now every term in the sum has either $\chi(g) = 0$ or $p|\chi(1)$, so it is divisible by p. Thus p divides 1, a contradiction. □

Theorem 151 (Burnside's p^aq^b theorem (1904))

If $|G| = p^aq^b$, then G is not a nonabelian simple group. (In particular, this means G must be solvable.)

Proof. Let P be a p-Sylow subgroup of G. Then P has nontrivial center, since P can be written as a union of $Z(G)$ and noncentral conjugacy classes. For any $x \in Z(P)$, the index of the centralizer $|\mathcal{C}_x| = [G : C(x)]$ contains P, so $[G : C(x)]$ must divide q^b. This is a contradiction to Theorem 150. □

It turns out that $z \in Z(G)$ if and only if $z \in Z(\chi)$, so we can look at the character table to deduce which elements are in the center. And we can also similarly pick out the derived group just by looking at characters, so the moral is that those characters do encode a lot of information about the group.

28 March 17, 2023

In this last lecture, we'll see a bit of how commutative algebra and representation theory can be tied together – we'll discuss **Galois group representations**, stating some results without proof. We'll start with a bit more finite group theory:

Definition 152
A finite group E is **elementary** if it is the direct product of a p-group and an abelian group.

Proposition 153
If E is elementary, then every irreducible representation of E is induced from a one-dimensional representation by some subgroup (called an M-group).

The M in M-group stands for "monomial" – it means that we can choose a basis of the representation so that the group elements are represented by monomial matrices.

Theorem 154 (Brauer, theorem A)
Any generalized character of a finite group G is a $\mathbb{Z}$-linear combination of characters induced from elementary subgroups.

In particular, by Proposition 153, we can always induce from one-dimensional characters of elementary subgroups. And this result has applications to Artin L-functions (which we'll see later on).

Theorem 155 (Brauer, theorem B)
A class function on G is a generalized character if and only if $\chi|_E$ is a generalized character for every elementary subgroup E of G.

This result has different-looking applications than the previous version – in particular, it can be used to compute the irreducible representations of GL_n. Brauer proved these results early on, and then Brauer and Tate came up with a clever proof afterward – the idea is to consider the ring X of generalized characters on G and let U be the set of all class functions χ with $\chi|_E$ a generalized character for every elementary subgroup E and V be the set of all generalized characters that are $\mathbb{Z}$-linear combinations of characters induced by elementary subgroups. We have $U \supseteq X \supseteq V$ – theorem A then claims that $X = V$ and theorem B then claims that $X = U$. But V is an ideal in U, so if we can prove that $1 \in V$ then $V = U$ and both theorems are implied.

We'll now turn to some commutative algebra, considering a familiar situation: let E/F be a finite separable extension of degree n, $A \subset F$ a Dedekind domain, and B the integral closure of A in E (which is also a Dedekind domain). If we let $\wp$ be a maximal ideal of A, then we can factor $\wp B$ into prime ideals in B as

$$\wp B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r},$$

where the $\mathfrak{P}_i$ are the prime ideals of B above A and we call e_i the **ramification index** of $\mathfrak{P}_i$. If we then define the **residue class degree** $f_i = [(B/\mathfrak{P}_i) : (A/\wp)]$, it turns out (we can consult Lang's algebraic number theory book) that $\boxed{\sum e_i f_i = n}$. In the case where $B = A[\alpha]$ (for example if $A = \mathbb{Z}$ and E is a cyclotomic field) this is easy to prove,

though some combination of localization and working with completions gives us the result in general as well. The idea is to let $f \in A[x]$ be an irreducible polynomial with root α; we can factor its image $\overline{f} \in A/\wp[x]$ into irreducible polynomials $\prod g_i^{e_i}$, where the e_is are again the ramification indices from above and where $\deg(g_i) = f_i$. And the idea is that if we look at a root β_i of g_i in some integral extension of $A/\wp$, then we can consider the homomorphisms $B : A[\alpha] \to \overline{A/\wp}$ sending α to β_i, which has kernel $\mathfrak{P}_i$. So we can use this to get a handle on the decomposition of $\wp B$ as a product of primes.

Example 156

Let $A = \mathbb{Z}$ and $B = A[\alpha]$ for some root α of $x^3 - 2$. Then if $\mathfrak{p} = (5)$, then $(x^3 - 2)$ factors mod 5 into $(x+2)(x^2+3x+4)$, so $\mathfrak{P}_1$ is the kernel of the homomorphism sending α to -2 (with $f_1 = 1$) and $\mathfrak{P}_2$ is the kernel of the homomorphism sending α to x^2+3x+4 in $\mathbb{F}_{5^2}$ (with $f_2 = 2$). Then indeed $f_1 + f_2 = 3$ with $e_1, e_2 = 1$ (no ramification).

Proposition 157

We will have all $e_i = 1$ unless $\overline{f}$ has a multiple root, meaning $\wp$ divides the discriminant $\prod(\alpha_i - \alpha_j)^2 \in A$. Since this discriminant only has a finite number of prime factors, this means there are always only finitely many $\wp$ that ramify, and other than that we just have $e_i = 1$ ("unramified primes").

It turns out that having one extension of degree 1 and one extension of degree 2, as in our example above, can't happen if we have a Galois extension:

Theorem 158

Suppose E/F is **Galois**. Then all e_i are equal and all f_i are equal.

The idea is that we can reduce to the case where $B = A[\alpha]$, and we notice that all roots of f will be in B. Since f is irreducible, the Galois group of E/F acts transitively on the roots of f. Thus the action is also transitive on the $\mathfrak{P}_i$s, and thus the residue class degrees and ramification indices must be all equal.

Example 159

Modifying the example above (with $A = \mathbb{Q}$ and $B = \mathbb{Q}(\alpha)$), if we adjoin all cube roots of 2 instead of just α, we get $C = \mathbb{Q}(\alpha, e^{2\pi i/3})$ (which is Galois over $\mathbb{Q}$); we have $\wp = \mathfrak{P}_1\mathfrak{P}_2$ as before (of $f_1 = 1, 2$ respectively). But then $\mathfrak{P}_1$ lifts to $\mathfrak{P}_1'$ in C with degree 2, and $\mathfrak{P}_2$ lifts to $\mathfrak{P}_2', \mathfrak{P}_3'$ each with degree 1. Thus $5C = \mathfrak{P}_1'\mathfrak{P}_2'\mathfrak{P}_3'$ with all $e_i = 1$ and all $f_i = 2$.

So if E/F is Galois and we assume all $e_i = 1$ and all $f_i = f$, we have

$$\wp B = \mathfrak{P}_1 \cdots \mathfrak{P}_r, \quad rf = [E : F] = n.$$

As we vary the prime $\wp$, we can get various behavior (for example, we may have $f = 1$ and the prime splits completely, or $r = 1$ and the prime stays prime). But if we let $D_{\mathfrak{P}_1} \subset \mathrm{Gal}(E/F)$ be the stabilizer of $\mathfrak{P}_1 = \mathfrak{P}$, also known as the **decomposition group**, we see that $D_{\mathfrak{P}_1}$ is conjugate to $D_{\mathfrak{P}_i}$ for all i, meaning that the decomposition group is determined up to conjugacy. (In particular, this means it is unique for an abelian extension.)

If we now assume that $A/\wp$ is **finite**, meaning we also have $B/\mathfrak{P}$ finite with $[(B/\mathfrak{P}) : (A/\wp)] = F$, then the Galois group $\mathrm{Gal}((B/\mathfrak{P})/(A/\wp))$ cyclic and generated by the **Frobenius element** $\sigma \mapsto \sigma^q$, where $q = |A/\wp|$ is the size of the

finite field (and thus $B/\mathfrak{P} = q^f$). We then get a homomorphism $D \to \mathrm{Gal}((B/\mathfrak{P})/(A/\wp)) = \mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$, which is surjective. Furthermore, having a nontrivial kernel comes from a ramification index not being 1, which we've assumed to not be the case, so we in fact have an isomorphism $D \cong \mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$.

Example 160

Suppose $A = \mathbb{Z}$ and $E = \mathbb{Q}(\zeta_N)$, where ζ_N is a primitive Nth root unity. Then it can be shown that $B = A[\zeta]$, and the generator of the Galois group is $\mathfrak{p}$ any prime not dividing N (that is, any unramified prime).

Then because $\mathrm{Gal}(E/F)$ is abelian and the decomposition group and Frobenius element are independent of the choice of prime above $\wp = (\mathfrak{p})$, we have $\phi_\wp \in \mathrm{Gal}(E/F)$ given by $\phi_p(\zeta) = \zeta^p$. So the Galois group is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$ (containing $\phi(N)$ elements), f is the order of p in $(\mathbb{Z}/N\mathbb{Z})^\times$, and $r = \frac{n}{f}$. And in the general case where we don't assume that the Galois group is abelian (but still avoid ramification), the Frobenius element in the Galois group is only determined up to conjugacy by $\phi(x) = x^q \mathrm{mod}\ \mathfrak{P}_i$.

So in short, every prime of the ground ring yields a conjugacy class of elements in the Galois group. And now we can see an application of Brauer's theorem:

Definition 161

Let F be a number field (that is, a finite extension of $\mathbb{Q}$), E/F a finite Galois extension, and A be the integral closure of $\mathbb{Z}$ in F. Let $G = \mathrm{Gal}(E/F)$ and $\pi : G \to \mathrm{GL}(V)$ a complex representation of G. The **Artin L-function** is defined via

$$L(s, \pi) = \prod_{\wp \text{ primes of } A} \left(1 - \frac{\chi(\phi_\wp)}{N\wp^s}\right)^{-1},$$

where $N\wp = |A/\wp|$. (The definition should be modified at ramified primes, but we're ignoring that for now.)

In the simplest case where $E = F = \mathbb{Q}$, this is just the usual Riemann zeta function. It was believed by Artin that just like the ordinary Riemann zeta function, we have functional equations and analytic continuations. Cases of this did eventually get proved, but the first important result was due to Brauer:

Theorem 162 (Brauer)

$L(s, \pi)$ is meromorphic.

In the cyclotomic case, this works out rather elegantly, using the fact that $1 - x^f = \prod_\varepsilon (1 - \varepsilon x)$ where we take the product over the fth roots of 1. And being entire is a consequence of the Langlands conjecture, in the case where $V^G = 0$ – the idea is that this should agree with the L-function of an automorphic form.

To sketch the idea here, the case where π is one-dimensional is known by work of Dirichlet and Hecke of 1919 (expressing in an integral form and then using Poisson summation). Then the idea is that **induction does not change the Artin L-function** (that is, if we have some subgroup H of G, which by the Galois correspondence corresponds to an intermediate field K, then $L(s, \pi)$ over K is the same as $L(s, \pi^G)$ over F). So now we can use Brauer's theorem to write χ as a linear combination of induced representations from one-dimensional representations, which proves the result.