Math 221 - Algebra

Taught by Héctor Pastén
Notes by Dongryul Kim

Fall 2016

The course was taught by Héctor Pastén this semester, and we met on Mondays, Wednesdays, and Fridays from 11:00am to 12:00pm. The textbooks we used were *Introduction to Commutative Algebra* by Atiyah and MacDonald, and *Representation theory: A first course* by Fulton and Harris. There were technically 12 students enrolled according to the Registrar. There was one take-home final exam and no course assistance.

Contents

1 August 31, 2016

This course will have four themes. The first one is commutative algebras: rings, modules, finitely generated modules, Noetherian modules, local rings, etc. The second one is Galois theory, and we will do some review to make sure everyone is on the same page. The third one is representations of finite groups. The way to know about a group is to see how it acts one stuff, and we only know linear algebra. So we deal with how the group acts on vector spaces. The fourth theme is Lie groups, which is a very large group. You would also want to look at the representation of the group, but this is too big. So you look at the tangent vector groups and get something called a Lie algebra, which is somewhere between the algebra and the geometry.

We won't have an in-class midterm, and there will be a take-home final exam. You can collaborate on assignments, although you would have to put some effort before asking. But you are not allowed to collaborate on the final exam.

1.1 Rings

Definition 1.1. A **ring** is a set A with two binary operations $+$, $\cdot$, and an element $0 \in A$ such that

(1) $(A; 0, +)$ is an abelian group,

(2) $\cdot$ is associative,

(3) $\cdot$ is distributive over $+$ (both from the right and the left).

We further say that A is **commutative** if $\cdot$ is commutative, and A is **unitary** if there is an element $1 \in A$ such that $1 \cdot x = x \cdot 1 = x$ for each $x \in A$.

For some time, we will use "ring" to mean a "commutative unitary ring". Also, most of the time, $A \neq \{0\}$.

Definition 1.2. For rings A and B, a function $f : A \to B$ is called a **ring morphism (map)** if f preserves $+$, $\cdot$, and 1.

Example 1.3. The map $f : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ with $n \mapsto (n, 0)$ is *not* a ring morphism.

One remark is that rings with there morphisms form a category. Still it is not the nicest category because there is no obvious struction on $\mathrm{Mor}(A, B)$. A ring morphism $f : A \to B$ is an isomorphism if and only if f is bijective. This is a property, not a definition. For instance, in the category of smooth maps, a map might be bijective but not be an isomorphism.

Definition 1.4. For a ring A, we define

$$A^\times = \{x \in A : xy = 1 \text{ for some } y \in A\} \subseteq A^* = A \setminus \{0\}.$$

The elements of $A^\times$ are called **units** of A.

When $A^\times = A^*$, we say that A is a **field**.

Definition 1.5. An element $x \in A$ such that $xy = 0$ for some $y \in A^*$ is called a **zero devisor**. If 0 is the only zero divisor, we say that A is an **(integral) domain**.

1.2 Ideals

Definition 1.6. Let A be a ring. An ideal of A is a subset $\mathfrak{a} \subseteq A$ such that

(1) $\mathfrak{a}$ is a subgroup of $(A; 0, +)$,

(2) $\mathfrak{a}A \subseteq \mathfrak{a}$ (which is equivalent to $\mathfrak{a}A = \mathfrak{a}$).

You can take quotients with ideals.

Proposition 1.7. *Let A be a ring and $\mathfrak{a} \subseteq A$ be an ideal. There is a unique ring structure in the quotient group $A/\mathfrak{a}$ such that the quotient map $\pi_\mathfrak{a} : A \to A/\mathfrak{a}$ is a ring morphism.*

Let $S \subseteq A$ be a subset. The **ideal generated by** S is

$$(S) = \text{the smallest ideal of } A \text{ containing } S.$$

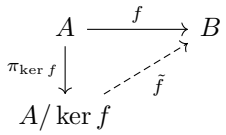
To show the existence, you take all the ideals containing S and intersect them. You can easily check that arbitrary intersections of ideals is an ideal. On the other hand, arbitrary unions of ideals is not necessarily an ideal. The right statement is that nested union of ideals is an ideal.

But this construction of (S) is not what you learn first. In kindergarten, you take the span. In fact (S) can also be constructed as

$$(S) = \{\textstyle\sum_{\text{finite}} s_j \alpha_j : s_j \in S, \alpha_j \in A\}.$$

Let $f : A \to B$ be a ring morphism. The image $\operatorname{im}(f)$ is naturally a subring, and the kernel $\ker(f)$ is naturally an ideal. The universal property of the kernel still holds for rings.

Proposition 1.8. *Let A be a ring. For any ring morphism $f : A \to B$, there exists a unique map $\tilde{f} : A/\ker f \to B$ such that $\tilde{f} \cdot \pi_{\ker f} = f$.*



Proposition 1.9. *Let $\mathfrak{a}$ be an ideal in A. There is a monotone bijection between the ideals containing $\mathfrak{a}$ and the ideals of $A/\mathfrak{a}$.*

$$\left\{\begin{matrix}\mathfrak{b} \subseteq A : \\ \mathfrak{a} \subseteq \mathfrak{b}\end{matrix}\right\} \quad \longleftrightarrow \quad \left\{\begin{matrix}\textit{ideals } \mathfrak{c} \\ \textit{of } A/\mathfrak{a}\end{matrix}\right\}$$

2 September 2, 2016

The last thing we discussed the bijection between the ideals of $A/\mathfrak{a}$ and the ideals of A containing $\mathfrak{a}$.

$$\begin{aligned} \{\text{ideals } A/\mathfrak{a}\} &\longleftrightarrow \left\{ \begin{matrix} \text{ideals in } A \\ \text{containing } \mathfrak{a} \end{matrix} \right\} \\ \mathfrak{b} &\longmapsto \pi_{\mathfrak{a}}^{-1}(\mathfrak{b}) \\ \pi_{\mathfrak{a}}(\mathfrak{c}) &\longmapsfrom \mathfrak{c} \end{aligned}$$

In this case, we got lucky, because an image of an ideal under $f : A \to B$ is not necessarily an ideal. At least when f is surjective this is true because it is a quotient. To this to be true, f has to bijective because $f(A)$ needs to be both a subring and an ideal of B. So this works only in this case.

2.1 Operation on rings and ideals

If $\mathfrak{a}, \mathfrak{b} \subseteq A$ are ideals, we define the following operations.

$$\begin{aligned} \mathfrak{a} + \mathfrak{b} &= \{\alpha + \beta : \alpha \in \mathfrak{a}, \beta \in \mathfrak{b}\}, \\ \mathfrak{a} \cdot \mathfrak{b} &= (\{\alpha \cdot \beta : \alpha \in \mathfrak{a}, \beta \in \mathfrak{b}\}). \end{aligned}$$

When we take only the elements that are products, you don't get an ideal.

Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are called **coprime** if $\mathfrak{a} + \mathfrak{b} = (1)$. This does not require unique factorization or anything.

For rings A_i for $i \in I \neq \emptyset$, we define the **product ring** as

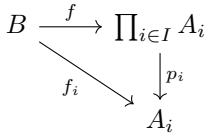
$$\prod_{i \in I} A_i = \{(\sigma : I \to \bigcup A_i) : \sigma(i) \in A_i \text{ for each } i \in I\}.$$

We are not assuming any cofinality of any sort. When I is finite the elements will look like tuples. Addition and multiplication will be defined element-wise.

There is a natural projection map

$$\begin{aligned} p_i : \prod_{i \in I} A_i &\to A_i \\ \sigma &\mapsto \sigma(i). \end{aligned}$$

This satisfies the universal property of the product. For any ring B and maps $f_i : B \to A_i$, there is a unique map $f : B \to \prod_{i \in I} A_i$ such that $f_i = p_i \circ f$ for all i.



What about the direct sum of rings? One cautionary remark is that the obvious thing to do, which is what you do for groups, doesn't work. The maps $A_i \to \text{“}\bigoplus A_i''$ maps 1 to something like $(\ldots, 0, 1, 0, \ldots)$ and therefore is not a morphism. Furthermore, if you take the direct sum of infinitely many rings, then you can't define 1. The right notion is the tensor product, which we will do soon.

Theorem 2.1 (Chinese remainder theorem)**.** *Let A be a ring and $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subseteq A$ be ideals. Define the map*

$$\phi : A \to \prod_{i=1}^{n} A/\mathfrak{a}_i.$$

in the obvious way. Then $\ker \phi = \bigcup_{i=1}^{n} \mathfrak{a}_i$ and ϕ is surjective if and only if $\mathfrak{a}_i + \mathfrak{a}_j = (1)$ for every $i \neq j$.

The proof is left as an exercise.

2.2 Prime and maximal ideals

Definition 2.2. Let A be a ring and $\mathfrak{a} \subsetneq A$ is an ideal.

(1) The ideal $\mathfrak{a}$ is **prime** if for any $x, y \in A$, $xy \in \mathfrak{a}$ implies $x \in \mathfrak{a}$ or $y \in \mathfrak{a}$.

(2) The ideal $\mathfrak{a}$ is **maximal** if for any ideal $\mathfrak{b} \subseteq A$, $\mathfrak{a} \subseteq \mathfrak{b}$ implies $\mathfrak{a} = \mathfrak{b}$ or $\mathfrak{b} \subseteq A$.

Proposition 2.3. *The ideal $\mathfrak{a}$ is prime if and only if $A/\mathfrak{a}$ is a domain. The ideal $\mathfrak{a}$ is maximal if and only if $A/\mathfrak{a}$ is a field.*

Proof. You can check this using the fact that the ideals of $A/\mathfrak{a}$ corresponds to ideals of A containing $\mathfrak{a}$. □

Now we get to the first theorem.

Theorem 2.4 (Krull, 1929)**.** *Let $\mathfrak{a} \subsetneq A$ be an ideal. There is a msximal ideal $\mathfrak{m} \subseteq A$ such that $\mathfrak{a} \subseteq \mathfrak{m}$.*

Proof. Consider the set

$$\mathcal{X}_{\mathfrak{a}} = \{\mathfrak{b} \subsetneq A \text{ ideal} : \mathfrak{a} \subseteq \mathfrak{b}\}$$

ordered by $\subseteq$. This is nonempty since $\mathfrak{a}$ is in it, and chains are bounded. Therefore by Zorn's lemma there exists a maximal element. □

2.3 Radicals

Definition 2.5. Let $A \neq (0)$. We define the **Jacobson radical** $\mathfrak{J}(A)$ and the **nilradical** $\mathfrak{N}(A)$ as

$$\mathfrak{J}(A) = \bigcap_{\mathfrak{m} \text{ maximal}} \mathfrak{m}, \qquad \mathfrak{N}(A) = \bigcap_{\mathfrak{p} \text{ prime}} \mathfrak{p}.$$

Proposition 2.6. *An element x is in $\mathfrak{J}(A)$ if and only if $1-xy \in A^\times$ for every $y \in A$.*

Proof. You can do this. □

Proposition 2.7. *An element x is in $\mathfrak{N}(A)$ if and only if x is nilpotent, i.e., $x^n = 0$ for some $n \geq 1$.*

Proof. For the $\Leftarrow$ direction, you note that $0 \in \mathfrak{p}$ for any prime $\mathfrak{p}$. Then by the definition of a prime, you see that $x^m \in \mathfrak{p}$ implies $x \in \mathfrak{p}$.

For the $\Rightarrow$ direction, suppose that x is not nilpotent. Consider the set

$$\Sigma_x = \{\mathfrak{a} \subseteq A : x^n \notin \mathfrak{a} \text{ for all } n \geq 1\}.$$

We check that $(0) \in \Sigma_x$ so it is nonempty. Also, chains are bounded because the union of the chain will also be in Σ_x. Therefore Zorn's lemma tells that there is a maximal element $\mathfrak{p}$.

We now claim that $\mathfrak{p}$ is prime. Note that $\mathfrak{p} \neq A$. Let $s, t \in A \setminus \mathfrak{p}$. It suffices to show that $st \in A \setminus \mathfrak{p}$. Observe that $\mathfrak{p} + (s), \mathfrak{p} + (t) \supsetneq \mathfrak{p}$. By the maximality of $\mathfrak{p}$, there exist $i, j \geq 1$ such that

$$x^i \in \mathfrak{p} + (s) \text{ and } x^j \in \mathfrak{p} + (t).$$

Then the product is $x^{i+j} \in \mathfrak{p} + (st)$ and therefore we get $st \notin \mathfrak{p}$ by the definition of Σ_x. □

One corollary is that the set of nilpotent elements in A is an ideal. You can to it directly, but you will do to do something like binomial expansion. Another corollary is that $A/\mathcal{N}(A)$ is reduced, i.e., the only nilpotent element is 0. In a similar vein, define the **radical** as

$$r(\mathfrak{a}) = \{x \in A : x^n \in \mathfrak{a} \text{ for some } n \geq 1\}.$$

Then $r(\mathfrak{a}) = \bigcap_{\mathfrak{a} \subseteq \mathfrak{p} \text{ prime}} \mathfrak{p}$.

3 September 7, 2016

3.1 Modules

Let A be a ring.

Definition 3.1. An **A-module** is an abelian group $(M, 0, +)$ together with a map $\cdot : A \times M \to M$ satisfying

(1) 1 acts as Id_M, i.e., $1 \cdot v = v$ for any $v \in M$,

(2) for every $\alpha, \beta \in A$ and $v \in M$, $(\alpha\beta)v = \alpha(\beta v)$,

(3) for every $\alpha, \beta \in A$ and $v \in M$, $(\alpha + \beta)v = \alpha v + \beta v$,

(4) for every $\alpha \in A$ and $v, w \in M$, $\alpha(v + w) = \alpha v + \alpha w$.

This is a generalization of the notion of vector spaces. If A is a field, A-modules are the same as A-vector spaces. If $A = \mathbb{Z}$, then A-modules are just abelian groups. To be precise, there is a forgetful functor from the category of $\mathbb{Z}$-modules to the category of abelian groups that is an equivalence. We also note that if $\mathfrak{a} \subseteq A$ is an ideal, then it is also an A-module.

We now define morphisms between A-rings. The definition requires the two modules to be over the same ring.

Definition 3.2. A **morphism of A-modules** is a morphism $f : M \to N$ of abelian groups which is A-linear, i.e., $f(\alpha v) = \alpha f(v)$.

One obvious remark is that for a fixed A, the A-modules with their morphisms form a category. In this category, isomorphisms are the same as bijective morphisms.

Unlike the case of rings, the set of morphisms $\mathrm{Hom}_A(M, N)$ from M to N inherits a structure of an A-module.

Example 3.3. Let M be an A-module. We define its dual module as

$$M^\vee = \mathrm{Hom}_A(M, A).$$

There is no reason for $M^\vee$ to be isomorphic to M. For instance, take $A = \mathbb{Z}$ and $M = \mathbb{Z}/2\mathbb{Z}$. Likewise, M and $M^{\vee\vee}$ are not isomorphic.

Example 3.4. Fix $f \in \mathrm{End}_A(M)$. Then we can make M into an $A[x]$-module by letting $x \cdot v = f(v)$. You need to be a bit careful here, because if I give you two endomorphisms $f, g \in \mathrm{End}_A(M)$, the A-module M inherits the structure of an $A[x, y]$-module only when f and g commutes.

3.2 Submodules and quotients

Although subrings are not what you really want to consider, submodules work quite well.

Definition 3.5. Let M be an A-module. A **submodule** N is a subgroup $N \leq M$ wich is an A-module with the A-action on M.

If $f \in \mathrm{Hom}_A(M,N)$, then $\ker f \leq M$ and $\mathrm{im}\, f \leq N$. You can take quotients, intersections, nested unions. You can also take the sums for a collection N_i of submodules of M as

$$\sum_{i\in I} N_i = \Big\{ \sum_{\text{finite}} v_i : v_i \in N_i \Big\}.$$

If $S \subseteq M$ is a subset, then we define the submodule generated by S as

$$\langle S \rangle = \bigcap_{S\subseteq N,\ N\leq M} N.$$

Also if M is and A-module and $\mathfrak{a} \subseteq A$ is an ideal, then we can define

$$\mathfrak{a}M = \{\textstyle\sum_{\text{finite}} \alpha_i v_i : \alpha_i \in \mathfrak{a}, v_i \in M\} \leq M.$$

The isomorphism theorems from group theory works the same for modules. You would need to check that the abelian group structure is compatible with scalar multiplication, but this is kind of obvious.

Proposition 3.6. *(1) Let $f \in \mathrm{Hom}_A(M,N)$. Then there exists a unique $\bar{f} \in \mathrm{Hom}_A(M/\ker f, N)$ such that $\bar{f} \circ q_{\ker f} = f$.*
(2) Let $P \leq N \leq M$ be A-modules. Then

$$(M/P)/(N/P) \cong M/N$$

(3) Let $N_1, N_2 \leq M$. Then

$$N_2/(N_1 \cap N_2) \cong (N_1 + N_2)/N_1$$

3.3 Direct sums and Direct products

Let M_i for $i \in I$ be A-modules. The **direct product** is defined as

$$\prod_{i\in I} M_i = \{\sigma : I \to \textstyle\bigcup_{i\in I} M_I : \sigma(i) \in M_i \text{ for all } i\}.$$

The **direct sum** is defined as

$$\bigoplus_{i\in I} M_i = \{\sigma : I \to \textstyle\bigcup_{i\in I} M_i : \sigma(i) \in M_i \text{ for all } i \text{ and has finite support}\}.$$

There are natural maps $p_i : \prod M_j \to M_i$ which is the projection and $\iota_i : M_i \to \bigoplus M_j$ which is extension by zero.

There are universal properties.

Proposition 3.7 (Universal property of the product)**.** *Let N be an A-module. For every collection of $f_i \in \mathrm{Hom}_A(N, M_i)$ there is a unique $f \in \mathrm{Hom}_A(N, \prod M_i)$ such that $f_i = p_i \circ f$ for all $i \in I$.*

Proposition 3.8 (Universal property of the direct sum)**.** *Let N be an A-module. For every collection of $g_i \in \mathrm{Hom}_A(M_i, N)$ there is a unique $g \in \mathrm{Hom}_A(\bigoplus M_i, N)$ such that $g_i = g \circ \iota_i$ for all $i \in I$.*

Here is a good exercise to do. Suppose you have another object that satisfies the same property. Using only this property, you can prove that what we have constructed and that other object must be isomorphic.

3.4 Other stuff about modules

Let M be an A-module. We define the **annihilator** of M as

$$\mathrm{Ann}(M) = \{\alpha \in A : \alpha \cdot M = \{0\}\}.$$

This is an ideal. We remark that M is an $A/\operatorname{Ann}(M)$-module in a natural way, and that it is faithful:

$$\mathrm{Ann}_{A/\operatorname{Ann}(M)}(M) = (0) \subseteq A/\operatorname{Ann}(M).$$

Definition 3.9. We say that M is **finitely generated** if there exists a finite subset $S \subseteq M$ such that $M = \langle S \rangle$.

Proposition 3.10. *M is finitely $M \cong A^n/K$ for $n \geq 0$ and $K \leq A^n$.*

Proof. Because M is finitely generated, there is some $S \subseteq M$ with S finite. Then we take $n = |S|$ and then there is a surjective map $A^n \to M$. Then we can quotient it out by the kernel of this map. □

We are going to need this lemma next class.

Lemma 3.11. *Let R be a ring and $T \in \mathcal{M}_{n\times n}(R)$ be a matrix with coefficients in R. There is another matrix $T' \in \mathcal{M}_{n\times n}(R)$ such that $T'T = \det(T) \cdot \mathrm{Id}$.*

We note that $\det T$ is well-defined as an element of R. As long as you don't divide, you can do linear algebra over a ring.

4 September 9, 2016

We were discussing finitely generated modules.

4.1 Nakayama's lemma

Proposition 4.1 (Cayley-Hamilton)**.** *Let M be a finitely generated A-module and $\mathfrak{a} \subseteq A$ be an ideal and $f \in \mathrm{End}_A(M)$ such that $f(M) \subseteq \mathfrak{a}M$. Then f satisfies an equation of the form*

$$f^n + \alpha_1 f^{n-1} + \cdots + \alpha_n = 0$$

with $\alpha_i \in \mathfrak{a}^i$, as a endomorphism of M.

Proof. Consider M as an $A[x]$-module with x acting as f. Let $v_1, \ldots, v_n \in M$ be the generators and let $\vec{v} = (v_i)_i \in \mathcal{M} = M^n$. Write $f(v_i) = \sum_j \beta_{ij} v_j$ with $\beta_{ij} \in \mathfrak{a}$ with some choice of β_{ij}.

Let $T = [\delta_{ij} x - \beta_{ij}]_{i,j} \in \mathcal{M}_{n\times n}(R)$ with $R = A[x]$. In more familiar terms, $T = Ix - [\beta_{ij}]$.

This $\mathcal{M}$ is an R-module with coordinate-wise action. Also T acts on $\mathcal{M}$ by matrix multiplication. The matrix T is chosen so that $T \cdot \vec{v} = 0$.

As in the previous lemma, there exists a matrix $T' \in \mathcal{M}_{n\times n}(R)$ such that $T'T = (\det T)I$. Then

$$(\det T)\vec{v} = (\det T)I\vec{v} = T'T\vec{v} = T'0 = 0.$$

Because v_i generate M, $\det T \in R$ annihilates M, i.e., acts as zero. Expanding $\det T$ gives the result. □

Many problems, like injectivity and surjectivity, reduces to knowing whether a module is the zero module.

Lemma 4.2 (Nakayama 1)**.** *Let M be a finitely generated A-module and let $\mathfrak{a} \subseteq A$ be an ideal. If $\mathfrak{a}M = M$ then there exists an $x \equiv 1 \pmod{\mathfrak{a}}$ such that $xM = 0$.*

Proof. Take $f = \mathrm{id}$. This is a hard choice because you don't expect this to give a nontrivial result. Apply Cayley-Hamilton. Then

$$x = 1 + \alpha_1 + \alpha_2 + \cdots + \alpha_n$$

acts as 0. □

Lemma 4.3 (Nakayama 2)**.** *Let M be a finitely generated A-module and let $\mathfrak{a} \subseteq A$ be an ideal. If $\mathfrak{a}M = M$ then there exists an $y \in \mathfrak{a}$ acting as* id *on M.*

Proof. Take $y = 1 - x$. □

Lemma 4.4 (Nakayama 3)**.** *Let M be a finitely generated A-module and $\mathfrak{a} \subseteq \mathfrak{J}(A)$. If $\mathfrak{a}M = M$ then $M = 0$.*

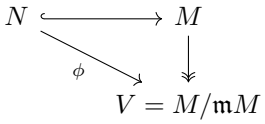
Proof. By Nakayama 1, there is an x such that $xM = 0$ and $1 - x \in \mathfrak{a} \subseteq \mathfrak{J}(A)$. Then x must be a unit. Then $0 = x^{-1}xM = M$. □

Lemma 4.5 (Nakayama 4)**.** *Let M be a finitely generated A-module and $\mathfrak{a} \subseteq \mathfrak{J}(A)$ be an ideal. If $N \leq M$ and $N + \mathfrak{a}M = M$ then $M = N$.*

Proof. Take the quotient module. □

Corollary 4.6. *Consider a local ring $(A, \mathfrak{m})$, i.e., $\mathfrak{m}$ is only the maximal ideal. Let M be a finitely generated module and $k = A/\mathfrak{m}$ be the residue field. The quotient $V = M/\mathfrak{m}M$ is a finite dimensional k-vector space. Let $v_1, \ldots, v_n \in M$ be lifts of the basis of V. Then $v_1, \ldots, v_n$ actually generate M.*

Proof. Let $N = \langle v_1, \ldots, v_n \rangle$. The composition ϕ of the inclusion $N \hookrightarrow M$ and the projection $M \to V$ must be surjective.

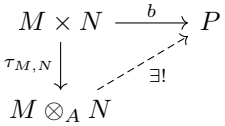


Because ϕ is surjective, $N + \mathfrak{m}M = M$. Since $\mathfrak{m} = \mathfrak{J}(A)$, we can apply Nakayama 4 and get the result. □

4.2 Tensor products

A **bilinear map** is a map $b : M \times N \to P$ such that for each $v \in M$, $b(v, -) \in \mathrm{Hom}_A(N, P)$ and for each $w \in N$, $b(-, w) \in \mathrm{Hom}_A(M, P)$.

Proposition 4.7. *Let M and N be A-modules. There exists an A-module $M \otimes_A N$ with a bilinear map $\tau_{M,N} : M \times N \to M \otimes_A N$ satisfying that for each bilinear $b : M \times N \to P$, there exists a unique map $b' \in \mathrm{Hom}_A(M \otimes_A N, P)$ such that $b = b' \circ \tau_{M,N}$.*



This $M \otimes_A N$ is called the **tensor product**. We also denote $\tau(v, w) = v \otimes w$. These pure tensors do not give all the elements of $M \otimes_A N$, but generate it.

These pure tensors satisfy many relations, so you always need to check whether a formula involving pure tensors actually gives a map from the tensor product. For instance in $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z}$,

$$1 \otimes 1 = 3 \otimes 1 = 1 \otimes 3 = 1 \otimes 0 = 0(1 \otimes 1) = 0.$$

In fact, you can show that $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} = 0$.

Proposition 4.8. *Tensor products have the following properties:*

(1) $A \otimes_A M \cong M$.

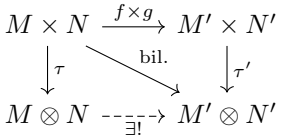
(2) $M \otimes_A N \cong N \otimes_A M$.

(3) $(M \otimes_A N) \otimes_A P \cong M \otimes_A (N \otimes_A P)$.

(4) Tensor products commute with arbitrary direct sums.

You can prove all these by using arrows, not pure tensors.

For maps $f \in \mathrm{Hom}(M, M')$ and $g \in \mathrm{Hom}(N, N')$, you can define a map $f \otimes g \in \mathrm{Hom}(M \otimes N, M' \otimes N')$. We can do this by using arrows.



For a ring A, an **A-algebra** is a ring B with a ring map $A \to B$. This is simply a ring that is also a A-module.

If M is an M-module and B is an A-algebra, then $M_B = B \otimes_A M$ is a B-module. This is because for any $x \in B$, multiplication by μ_x gives a map $\mu_x \otimes \mathrm{id} \in \mathrm{End}_A(B \otimes_A M)$. This gives $B \otimes_A M$ an B-module structure.

5 September 12, 2016

Last time we were talking about tensor products. For A-modules M and N, there is another module $M \otimes_A N$ with a universal bilinear map $\tau : M \times N \to M \otimes_A N$. The pure tensors are $v \otimes w = \tau(v, w)$. By bilinearity of τ, these pure tensors satisfies some relations. To construct $M \otimes_A N$, you can write down all the pure tensors, construct the free A-module generated by them, and then quotient by the submodule generated the relations. This way, you kill exactly what you need to be zero, and so it satisfies the universal property.

Given two maps $f : M \to N$ and $g : M' \to N'$, there is a map

$$\begin{aligned} f \otimes g : M \otimes_A M' &\to N \otimes_A N' \\ v \otimes w &\mapsto f(v) \otimes g(w). \end{aligned}$$

This is actually well-defined, because you can describe it through the universal property.

$$\begin{array}{ccc} M \times M' & \xrightarrow{f \times g} & N \times N' \\ \downarrow{\scriptstyle \tau} & \searrow & \downarrow{\scriptstyle \tau} \\ M \otimes_A M' & \dashrightarrow & N \otimes_A N' \end{array}$$

Suppose you have an A-module M and an A-algebra B. An A-algebra is just a ring B with a map $\psi : A \to B$. This map allows B to be seen as an A-module, because for $\alpha \in A$ and $\beta \in B$, we can define $\alpha \cdot \beta = \psi(\alpha) \cdot_B B$. Now you want to make M into a B-module. Why would you want to do that? Suppose that you have a linear algebra problem but are working in the reals. You want to look at the eigenvalues but there might exist no eigenvalues in the reals. So you work in the complex numbers for a while. This is extending the scalar.

Define $M_B = B \otimes_A M$. We can give a B-module structure on $B \otimes_A M$ as $\beta(\gamma \otimes v) = (\beta\gamma) \otimes v$. Why is this well-defined? That map can be described as the tensor product of the multiplication map $\mu_\beta : B \to B$ and $\mathrm{id} : M \to M$. Then

$$(\mu_\beta \otimes \mathrm{id})(\gamma \otimes v) = (\mu_\beta(\gamma) \otimes v) = (\beta\gamma) \otimes v.$$

These actions of B on M_B gives a map $B \times M_B \to M_B$ given by

$$(\beta, x) \mapsto (\mu_\beta \otimes \mathrm{id})(x).$$

5.1 Tensor products of algebras

There is a notion of tensor products of A-algebras. Let B and C be A-algebras. Let us look at $B \otimes_A C$ first as an A-module. Then this is $C_B \cong B_C$. But it is also a ring, because you can define

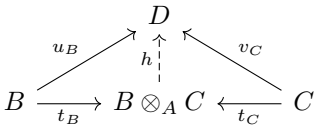
$$(\beta \otimes \gamma) \cdot (\beta' \otimes \gamma') = (\beta\beta') \otimes (\gamma\gamma').$$

The magic of this is that we have canonical ring maps $t_B : B \to B \otimes_A C$ and $t_C : C \to B \otimes_A C$ given by

$$t_B : \beta \mapsto \beta \otimes 1 = \beta(1 \otimes 1), \qquad t_C : \gamma \mapsto 1 \otimes \gamma = \gamma(1 \otimes 1).$$

These maps are good because they also respects multiplication. The data $(B \otimes_A C, \tau_{B,C}, t_B, t_C)$ has a universal property.

Proposition 5.1. *Let A be a ring and B, C be A-algebras. Let D be an A-algebra with A-algebra maps $v_B : B \to D$ and $v_C : C \to D$. Then there exists a unique A-algebra map $h : B \otimes_A C \to D$ such that*



commutes.

Proof. We first build a A-linear map $B \otimes_A C \to D$. To get this, we need a A-bilinear map $m : B \times C \to D$. We use the map given by

$$(\beta, \gamma) \to u_B(\beta) \cdot_D u_C(\gamma).$$

The map h is going to be unique map that factors m. This map h actually satisfies the diagram and so this shows existence of h. This does not quite prove uniqueness because this uniqueness of h coming from the universal property of tensor products is not quite the uniqueness we want. We first see that the image of pure tensors are determined. For any pure tensor $\beta \otimes \gamma = (\beta \otimes 1)(1 \otimes \gamma)$. Then $h(\beta \otimes 1) = u_B(\beta)$ and $h(\gamma \otimes 1) = u_C(\gamma)$. Then if you want h to be a ring map, then $h(\beta \otimes \gamma) = u_B(\beta)u_C(\gamma)$. This shows uniqueness. □

5.2 Free modules

We assume $A \neq (0)$ for the discussion of free modules. Let M be an A-module and $S \subseteq M$ be a subset. Then S is

(1) a **generating set** if $M = \langle S \rangle$,

(2) a **free set** if the elements of S only satisfy the trivial A-linear relation, and

(3) a **basis** if it is a generating set and a free set.

The module M is a **free A-module** if it has a basis.

Example 5.2. Take $A = \mathbb{Z}$. Then $M = \mathbb{Z}$ is a free module with basis $\{1\}$. The set $S = \{2, 3\}$ is a generating set but not a free set. Although this is a minimal generating set, it is not a basis. The module $M = \mathbb{Z}/2$ is not free because it has no nonempty free set.

Proposition 5.3. *A module M is free with basis $\{x_i\}_{i \in I}$ if and only if $M \cong A^{(I)}$ where $A^{(I)}$ denotes A direct summed I times.*

6 September 14, 2016

Last time we were discussing free modules. Every free module is nothing but $A^{(I)}$ up to isomorphism. Still this does not trivializes the theory of free modules.

Proposition 6.1. *Let M be a free A-module and let S be a basis for M. Given any A-module N and a set map $\sigma : S \to N$, there is a unique A-module map $f \in \mathrm{Hom}_A(M, N)$ with $f|_S = \sigma$.*

This is just linear algebra.

6.1 Rank of a free module

Proposition 6.2. *Let B be an A-algebra. If M is a free A-module with basis $\{x_i\}_{i\in I}$, then M_B is a free B-module with basis $\{1_B \otimes x_i\}_{i\in I}$.*

Proof. Consider the case of $A^{(I)}$ with $x_i = e_i$. The result follows from that tensor product commutes with arbitrary direct sum. □

Proposition 6.3. *There is an isomorphism $A^{(I)} \cong A^{(J)}$ if and only if $|I| = |J|$.*

Proof. Let $m \subseteq A$ be a maximal ideal. Tensor with $A/\mathfrak{m}$. Then $(A/\mathfrak{m})^{(I)} \cong (A/\mathfrak{m})^{(J)}$ and this is now just linear algebra. □

Definition 6.4. Let M be a free module. The **rank** of M is defined as the cardinal $\mathrm{rk}_A M = |I|$ for I satisfying $M \cong A^{(I)}$.

Proposition 6.5. *Let M be a free A-module of* finite rank $r = \mathrm{rk}_A M$.

(1) Every set of r generators is a basis.

(2) Every set of generators has at least r elements.

Proof. (a) Let $\{x_i\}_{i=1}^r$ be a generating set. Let $\{v_1\}_{i=1}^r$ be a basis. Consider $\sigma : \{v_i\} \to M$ mapping $v_i \mapsto x_i$. By the universal property, there uniquely exists $f \in \mathrm{End}_A M$ such that $f : v_i \mapsto x_i$. Note that f is surjective. By Nakayama, f is an isomorphism. □

For M and N of finite rank, clearly $\mathrm{rk}_A(M \oplus N) = \mathrm{rk}_A M + \mathrm{rk}_A N$. Also $\mathrm{rk}_A(M \otimes N) = \mathrm{rk}_A M \cdot \mathrm{rk}_A N$.

6.2 Direct limits

Consider a poset $(I, \leq)$ such that for every $i, j \in I$ there exists $k \in I$ with $i, j \leq k$. (This is usually known as a **filtered**.) We are going to call this a **directed set**.

Given a direct set I, a **direct system** of A-modules is a pair $(\{M_i\}_{i\in I}, \{\mu_{ij}\}_{i,j\in I, i\leq j})$ with

- $\mu_{ij} : M_i \to M_j$ (or $\mu_{ij} \in \mathrm{Hom}_A(M_i, M_j)$)

- $\mu_{ij} = \mu_{kj} \circ \mu_{ij}$ for any $i \leq k \leq j$.

We construct the direct limit of this system in the following way. Take

$$\varinjlim M_i = \oplus M_i / D \text{ where } D = \langle \{\iota_i(x_i) - \iota_j(\mu_{ij}(x_i)) : i \leq j, x_i \in M_i\}\rangle$$

that comes with the natural maps

$$\mu_j = p_D \iota_j : M_j \to \varinjlim M_j.$$

We call $(\varinjlim M_i, \{\mu_i\}_{i\in I})$ the **direct limit** of the system. We have compressed the information of the system into this.

Proposition 6.6 (Universal property of the direct limit)**.** *Let $(\{M_i\}, \{\mu_{ij}\})$ be a direct system. For any A-module N with maps $f_i \in \mathrm{Hom}_A(M_i, N)$ satisfying $f_i = f_j \mu_{ij}$ (for all $i \leq j$) there exists a unique $f \in \mathrm{Hom}_A(\varinjlim M_i, N)$ such that $f_i = f\mu_i$ for all i.*

This is built out of two universal property: that of the direct sum, and that of the quotient.

Let M be an A-module. Consider

$$I = \{N \leq M : N \text{ is finitely generated }\}$$

which is a poset by inclusion and is also filtered because the sum of finitely generated modules is finitely generated.

Proposition 6.7. *With M and I as above, we have $M \cong \varinjlim M_i$ where $M_i = i$.*

This is a powerful tool because if you see that some property is preserved under direct limits, and you know it is true for finitely generated modules, then you can conclude that it is true for all modules.

Proof. Check that $(M, \{M_i \hookrightarrow M\})$ satisfies the universal property. □

Proposition 6.8. *Let $(M_i, \{\mu_{ij}\})$ be a direct system and let N be an A-module. Then*

$$(\varinjlim M_i) \otimes N \cong \varinjlim (M_i \otimes N).$$

Proof. For eveyr i, there is a map $\tau : M_i \times N \to M_i \otimes N$. Apply $\varinjlim$ and we get a map $\tau : (\varinjlim M_i) \times N \to \varinjlim (M_i \otimes N)$ that is bilinear. So by the universal property of the tensor product, we get a map

$$\tau' : (\varinjlim M_i) \otimes N \to \varinjlim (M_i \otimes N).$$

Now let us get the other direction. For every i, we consider the map $\mu_i \otimes \mathrm{id} : M_i \otimes N \to (\varinjlim M_i) \otimes N$. Choose $f_i = \mu_i \otimes \mathrm{id}$. By the universal property, we get a map

$$\varinjlim_{\mu_{ij}\otimes \mathrm{id}} (M_i \otimes N) \to (\varinjlim M_i) \otimes N.$$

Check that they are inverses. □

Here is a useful construction of direct limit of morphisms. Consider two direct systems M_i and N_j on the same index set I, and maps $\phi_i : M_i \to N_i$ that are compatible with the direct system, i.e.,

$$\begin{array}{ccc} M_i & \xrightarrow{\phi_i} & N_i \\ \downarrow{\scriptstyle \mu_{ij}} & & \downarrow{\scriptstyle \mu'_{ij}} \\ N_j & \xrightarrow{\phi_j} & N_j \end{array}$$

commutes for all $i \leq j$. How do we compute $\varinjlim \phi_i$? We first compoes ϕ_j with the natural maps $N_i \to \varinjlim N_i$ to get the maps f_i. Then we can use the universal property to get $\varinjlim \phi_i$.

$$\begin{array}{ccc} M_i & \xrightarrow{\phi_i} & N_i \\ \downarrow{\scriptstyle \mu_i} & \searrow^{f_i} & \downarrow \\ \varinjlim M_i & \dashrightarrow & \varinjlim N_i \end{array}$$

This suggest that there is a functor from the category of directed systems to modules.

7 September 16, 2016

Today we are going to introduce two notions: flatness and localization.

7.1 Exactness and flatness

We say that a sequence

$$M \xrightarrow{f} N \xrightarrow{g} P$$

is **exact** if $\ker g = \operatorname{im} f$. A **short exact sequence** is a sequence

$$0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$$

that is exact at M, N, and P.

Proposition 7.1. *Let S be a sequence*

$$M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$$

of A-modules. Then the following are equivalent:

(i) S is exact.

(ii) For any L, the following sequence is exact.

$$0 \longrightarrow \operatorname{Hom}(P, L) \longrightarrow \operatorname{Hom}(N, L) \longrightarrow \operatorname{Hom}(M, L)$$

The functor $\operatorname{Hom}_A(-, L)$ is contravariant and $\operatorname{Hom}_A(L, -)$ is covariant. We then say that the functor $\operatorname{Hom}_A(-, L)$ is **left exact**, because the 0 is on the left after applying the functor. This is weaker than every exact sequence being sent to an exact sequence.

Proposition 7.2. *Let N be a A-module. If $S : M \to P \to Q \to 0$ is exact, then $M \otimes N \to P \otimes N \to Q \otimes N \to 0$ is exact.*

Proof. We apply the previous proposition. For every L, the sequence

$$0 \longrightarrow \operatorname{Hom}(Q, \operatorname{Hom}(N, L)) \longrightarrow \operatorname{Hom}(P, \operatorname{Hom}(N, L)) \longrightarrow \operatorname{Hom}(M, \operatorname{Hom}(N, L)).$$

is exact. There is a canonical isomorphism $\operatorname{Hom}(Q, \operatorname{Hom}(N, L)) \cong \operatorname{Bil}_A(Q \times N, L) \cong \operatorname{Hom}(Q \otimes N, L)$. Now use the previous proposition again. □

We note that the functor $- \otimes N$ is not always left exact. Consider the injection $\mathbb{Z} \to \mathbb{Z}$ given by multiplication by 2. If we tensor by $\mathbb{Z}/2\mathbb{Z}$, then we get $\mathbb{Z}/2 \to \mathbb{Z}/2$ that is also multiplication by two. This is not injective.

Proposition 7.3. *The functor $N \otimes_A -$ preserves injective maps if and only if it is exact.*

Definition 7.4. N is a **flat** A**-module** if $N \otimes -$ is exact.

For instance, $\mathbb{Z}/2$ is not a flat $\mathbb{Z}$-module.

Proposition 7.5 (See assignment)**.** *(1) The direct sum $\bigoplus M_i$ is flat if and only if each M_i is flat.*

(2) If M is a flat A-module and B is an A-algebra, then M_B is a flat B-module.

Example 7.6. A is a flat A-module. Free modules are flat, because it is a direct sum of flat modules. So $A[x]$ is a flat A-module, and vector spaces are flat k-modules.

Theorem 7.7. *For an A-module N, the following are equivalent:*

(1) N is flat.

(2) For every ideal $\mathfrak{a} \subseteq A$, the map $\mathfrak{a} \otimes_A N \to N$ is injective.

Proof. For (1) $\Rightarrow$ (2), we have an exact sequence $0 \to \mathfrak{a} \to A$. Then $0 \to \mathfrak{a} \otimes A \to A \otimes N \cong N$ is exact.

This is terribly complicated. See [Liu] Theorem 2.4. The other short proof uses Tor functors. □

7.2 Localization

Definition 7.8. A set $S \subseteq A$ is a multiplicative set if $1 \in S$ and S is closed under multiplication.

For example, $S = \{1, x, x^2, \ldots\}$ is a multiplicative set for any $s \in A$. The set $S = A \setminus \mathfrak{p}$ is also a multiplicative set for any prime ideal $\mathfrak{p}$.

Now let $S \subseteq A$ be a multiplicative set. On $A \times S$ define the relation

$$(\alpha, s) \sim (\beta t) \quad \Leftrightarrow \quad \exists r \in S \text{ such that } r(\alpha t - \beta s) = 0.$$

Then we define the **localization** $S^{-1}A = A \times S/\sim$. It can be verified that $S^{-1}A$ is a ring with the obvious formulas for $+$ and $\cdot$ (of fractions). We denote $\alpha/s = [(\alpha, s)]$.

It also comes with a natural map

$$\lambda_S : A \to S^{-1}A, \qquad \alpha \mapsto \alpha/1.$$

that is a ring map. Thus $S^{-1}A$ is an A-algebra in a natural way. This λ_S is called the **localization map**. The invertible elements are mapped to $\lambda_S(A^\times) \subseteq (S^{-1}A)^\times$, and also S is mapped into $\lambda_S(S) \subseteq (S^{-1}A)^\times$.

Proposition 7.9. *Let A be a ring and $S \subseteq A$ a multiplicative set. For all A-algebras $f : A \to B$ satisfying $f(S) \subseteq B^\times$, there exists a unique ring map $f' : S^{-1}A \to B$ with $f' \circ \lambda_S = f$.*

Proof. If you want a reference, this is [AM] Proposition 3.1. □

We denote $A_x = \{1, x, x^2, \ldots\}^{-1}A$ and $A_{\mathfrak{p}} = (A \setminus \mathfrak{p})^{-1}A$ for a prime ideal $\mathfrak{p} \subseteq A$.

There is also a module version for localization. Let A be a ring and $S \subseteq A$ be a multiplicative set. Let M be an A-module. We define $S^{-1}M = M \times S/\sim$ where the relation is defined by

$$(v, s) \sim (w, t) \quad \Leftrightarrow \quad \exists r \in S, r(tv - sw) = 0.$$

The resulting $S^{-1}M$ is an $S^{-1}A$-module, with the action given by $(\alpha/s)\cdot(v/t) = (\alpha v/st)$.

Again, this has a universal property. As an exercise, write down the universal property for $\lambda_{M,S} : M \to S^{-1}M$.

From a categorical point of view, the next thing we have to do is localization of morphisms. Let A be a ring and $S \subseteq A$ be a multiplicative set. For $f \in \mathrm{Hom}_A(M, N)$, we want to make $S^{-1}f \in \mathrm{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N)$. If we succeed, we realize S^{-1} as a functor from the category of A-modules to the category of $S^{-1}A$-modules. This is easy once we have the universal property for $S^{-1}A$-modules.

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \downarrow{\scriptstyle \lambda_{M,S}} & \searrow & \downarrow{\scriptstyle \lambda_{N,S}} \\ S^{-1}M & \underset{\exists! = S^{-1}f}{\dashrightarrow} & S^{-1}N. \end{array}$$

So $S-1$ defines a functor.

Theorem 7.10. *This functor is exact.*

Proof. Take any exact sequence

$$M \xrightarrow{f} N \xrightarrow{g} P$$

of A-modules. First we need to check that $\operatorname{im} f_S \subseteq \ker g_S$, but this is clear because $g \circ f = 0$ and then by localizing by S, we get $g_S \circ f_S = 0$.

To show $\operatorname{im} f_S \supseteq \ker g_S$, let $v/s \in \ker g_S$. Then $0 = g_S(v/s) = g(v)/s$, and so there exists and $r \in S$ such that $rg(v) = 0$. So $g(rv) = 0$ and $rv \in \ker g = \operatorname{im} f$. Let $rv = f(w)$ with $w \in M$. Then

$$f_s\Big(\frac{w}{rs}\Big) = \frac{f(w)}{rs} = \frac{rv}{rs} = \frac{r}{s}. \qquad \square$$

8 September 19, 2016

Let me talk a little bit more about localization.

Proposition 8.1. *Let $S \subseteq A$ be a multiplicative set and let M be an A-module the map $M_{S^{-1}A} = S^{-1}A \otimes_A M \to S^{-1}M$ by $(1/s) \otimes v \mapsto v/s$ is an isomorphism.*

Proof. There is a bilinear map $f : S^{-1}A \times M \to S^{-1}M$ given by $(\alpha/s, r) \mapsto \alpha v/s$. This gives a map $f' : S^{-1}A \otimes_A M \to S^{-1}M$ that is clearly surjective. You can check injectivity on elements. □

Corollary 8.2. *$S^{-1}A$ is a flat A-algebra.*

Corollary 8.3. *$S^{-1}(M \otimes_A N) \cong S^{-1}M \otimes_{S^{-1}A} S^{-1}N$.*

Proof. We have $S^{-1}M \otimes_{S^{-1}A} S^{-1}N \cong (M \otimes_A S^{-1}A) \otimes_{S^{-1}A} S^{-1}N$. By the bimodule property, the tensor product commutes and this is isomorphic to

$$\begin{aligned} M \otimes_A (S^{-1}A \otimes_{S^{-1}A} S^{-1}M) &\cong M \otimes_A S^{-1}A \cong M \otimes_A (N \otimes_A S^{-1}A) \\ &\cong (M \otimes_A N) \otimes_A S^{-1}A \cong S^{-1}(M \otimes_A N). \end{aligned}$$

□

Likewise, tensoring by a quotient has a natural interpretation. For any ideal $\mathfrak{a} \subseteq A$, there is an exact sequence

$$0 \longrightarrow \mathfrak{a} \longrightarrow A \longrightarrow A/\mathfrak{a} \longrightarrow 0.$$

Then we can tensor with M to get

$$\mathfrak{a} \otimes M \cong \mathfrak{a}M \longrightarrow A \otimes M \cong M \longrightarrow A/\mathfrak{a} \otimes M \longrightarrow 0.$$

This implies that $(A/\mathfrak{a}) \otimes M \cong M/\mathfrak{a}M$ naturally.

In a similar way, you can also get $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$.

8.1 Local properties

Proposition 8.4. *Let M be an A-module. The following are equivalent:*

(1) $M = 0$.

(2) $M_{\mathfrak{p}} = 0$ for all prime $\mathfrak{p} \subseteq A$.

(3) $M_{\mathfrak{m}} = 0$ for all maximal $\mathfrak{m} \subseteq A$.

Proof. It is obvious that (1) ⇒ (2) ⇒ (3). Let us now prove (3) ⇒ (1). Assume (3) with $M \neq 0$. There is an $0 \neq v \in M$, so $1 \notin \operatorname{Ann}_A(v)$. So there exists a maximal $\mathfrak{m}$ such that $\operatorname{Ann}_A v \subseteq \mathfrak{m}$.

Let us now look at $v/1 = 0$ in $M_{\mathfrak{m}} = 0$. There should be an $r \in A \setminus \mathfrak{m}$ such that $rv = 0$ in M. Then r is both in $\operatorname{Ann}_A(v)$ and $A \setminus \mathfrak{m}$ and so we get a contradiction. □

Proposition 8.5. *Let $f \in \mathrm{Hom}_A(M, N)$. The following are equivalent:*

(1) f is injective.

(2) $f_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ in injective for all prime $\mathfrak{p} \subseteq A$.

(3) $f_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective for all maximal $\mathfrak{m} \subseteq A$.

The same holds for "surjection" and "isomorphism".

Proof. (2) $\Rightarrow$ (3) is obvious. (1) $\Rightarrow$ (2) directly follows from that localization is exact. (3) $\Rightarrow$ (1) follows from the exactness of localization and the previous proposition. □

Proposition 8.6. *Let $N, P \leq M$ be A-modules. The following are equivalent:*

(1) $N \subseteq P$.

(2) $N_{\mathfrak{p}} \subseteq P_{\mathfrak{p}}$ for all prime $\mathfrak{p} \subseteq A$.

(3) $N_{\mathfrak{m}} \subseteq P_{\mathfrak{m}}$ for all maximal $\mathfrak{m} \subseteq A$.

The proof is an exercise.

Proposition 8.7. *Exactness of sequences is local.*

Proposition 8.8. *Flatness is local.*

Proof. (2) $\Rightarrow$ (3) is trivial. Let us prove (1) $\Rightarrow$ (2). Let M be a flat A-module. Then $A_{\mathfrak{p}} \otimes M$ is a flat $A_{\mathfrak{p}}$-module. But this is $M_{\mathfrak{p}}$ and so we are done.

Now we check (3) $\Rightarrow$ (1). Let $N \to P$ be an injective map of A-modules. We need to show that if (3) holds for M then $N \otimes_A M \to P \otimes_A M$ is injective. Because $N \to P$ is injective, $N_{\mathfrak{m}} \to P_{\mathfrak{m}}$ is also injective. Because $M_{\mathfrak{m}}$ is flat, $N_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} M_{\mathfrak{m}} \to P_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} M_{\mathfrak{m}}$ is injective for every $\mathfrak{m}$. Because the diagram

$$\begin{array}{ccc} N_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} M_{\mathfrak{m}} & \longrightarrow & P_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} M_{\mathfrak{m}} \\ \downarrow \cong & & \downarrow \cong \\ (N \otimes AM)_{\mathfrak{m}} & \longrightarrow & (P \otimes_A M)_{\mathfrak{m}} \end{array}$$

commutes. Then $N \otimes_A M \to P \otimes_A M$ is injective. □

An important cautionary remark is that freeness is not local. Locally free is not the same as free.

Theorem 8.9. *Let M be a finitely generated A-module. Then M is flat if and only if M is **locally free**, i.e., the following are equivalent:*

(1) M is a flat A-module.

(2) $M_{\mathfrak{p}}$ is a free $A_{\mathfrak{p}}$-module for each prime $\mathfrak{p} \subseteq A$.

(3) $M_{\mathfrak{m}}$ is a free $A_{\mathfrak{m}}$-module for each maximal $\mathfrak{m} \subseteq A$.

Proof. Use that flatness is local and problem 1 of assignment 4, which states that if A is a local ring then a finitely generated module is flat if and only if it is free. □

Proposition 8.10. *Let $S \subseteq A$ be a multiplicative set.*

(1) Every ideal of $S^{-1}A$ is of the form $(\lambda_S(\mathfrak{a}))$ for an ideal $\mathfrak{a} \subseteq A$.

(2) We have a monotone bijection:

$$\left\{ \begin{array}{c} \mathfrak{p} \subseteq A \text{ prime} : \\ S \cap \mathfrak{p} \neq \emptyset \end{array} \right\} \quad \longleftrightarrow \quad \operatorname{Spec} S^{-1}A = \{q \subseteq S^{-1}A \text{ prime}\}.$$

(3) S^{-1} respects the following operations on ideals: finite (not direct) sums, products, finite intersection, and radicals.

In the last three minutes, let me say a word on Spec.
For a ring A, we define

$$X = \operatorname{Spec} A = \{\mathfrak{p} \subseteq A : \mathfrak{p} \text{ prime}\}.$$

We want to do geometry here (on X) and we want to see elements of A as "functions" on X. We also want to see A-modules as sheaves of X. Later we are going to put a topology on X.

9 September 21, 2016

Today we are going to discuss primary decomposition.

9.1 Primary ideals

Definition 9.1. An ideal $\mathfrak{q} \subseteq A$ is **primary** if $xy \in \mathfrak{q}$ implies $x \in \mathfrak{q}$ or $y^n \in \mathfrak{q}$ for some $n \geq 1$. In other words, $\mathfrak{q}$ is primary if and only if $A/\mathfrak{q}$ has the property that all its zero divisors are nilpotent.

So maximal implies prime implies primary. For example, $(x^2) \subseteq k[x]$ is primary. If $f : A \to B$ is any ring morphism and $\mathfrak{q} \subseteq B$ is an ideal, then $\mathfrak{q}$ prime implies $f^{-1}\mathfrak{q}$ is prime. Likewise $\mathfrak{q}$ primary implies $f^{-1}(\mathfrak{q})$ is primary. This is not true for maximal ideals.

Proposition 9.2. *Let $\mathfrak{q} \subseteq A$ be an ideal.*

(1) If $\mathfrak{q}$ is primary, then $r(\mathfrak{q})$ is the smallest prime containing $\mathfrak{q}$.

(2) If $r(\mathfrak{q})$ is maximal, then $\mathfrak{q}$ is primary.

Proof. (1) It is enough to show that $r(\mathfrak{q})$ is prime, because $r(\mathfrak{q})$ is the intersection of all primes containing $\mathfrak{q}$. You can check it on elements.

(2) Say $\mathfrak{r}(q) = \mathfrak{m}$ is maximal. Then $\mathfrak{q} \subset \mathfrak{m}$, and so $\overline{\mathfrak{m}}$ is maximal in $A/\mathfrak{q}$, with

$$\overline{\mathfrak{m}} = \overline{r_A(\mathfrak{q})} = r_{A/\mathfrak{q}}(0) = \mathfrak{N}(A/\mathfrak{q}) = \bigcap_{\mathfrak{p} \subseteq A/\mathfrak{q}} \mathfrak{p}.$$

From this we conclude that $\overline{\mathfrak{m}}$ is the only maximal ideal.

Now let $x \in A/\mathfrak{q}$ be a zero divisor. Then (x) is contained in some maximal ideal, but $\overline{\mathfrak{m}}$ is the only maximal ideal. So $x \in \overline{\mathfrak{m}} = \mathfrak{N}(A/\mathfrak{q})$. So x is nilpotent. □

It is not hard to check that if there exists a maximal ideal $\mathfrak{m}$ such that $\mathfrak{m}^j = (0)$ for some j, then $\mathfrak{m}$ must be the only prime ideal.

Corollary 9.3. *Powers of maximal ideals are primary.*

Definition 9.4. Let $\mathfrak{q} \subset A$ be primary. We say $\mathfrak{q}$ is **$\mathfrak{p}$-primary** if $\mathfrak{p} = r(\mathfrak{f})$.

The way you want to think about this is that $\mathfrak{p}$ is a shadow of $\mathfrak{q}$.

Proposition 9.5. *Finite intersections of $\mathfrak{p}$-primary ideals is $\mathfrak{p}$-primary.*

This will be an exercise. On the other hand, it is not true (in general) that finite intersection of primary is primary. Here is an example. Let $A = k[x, y]$ and $\mathfrak{q}_1 = (x)$, $\mathfrak{q}_2 = (y)$. They are both primary, but their intersection is not primary.

Definition 9.6. Take $\mathfrak{a} \subseteq A$ be an ideal, and let $x \in A$. The **transporter** of x to $\mathfrak{a}$ is defined as

$$(\mathfrak{a} : x) = \{y \in A : yx \in \mathfrak{a}\}.$$

This is clearly an ideal. Using the quotient ring, we can also write $(\mathfrak{a} : x) = \operatorname{Ann}_A(x \bmod \mathfrak{a}) \subseteq A$. Also obviously $\mathfrak{a} \subseteq (\mathfrak{a} : x)$, and if $x \in \mathfrak{a}$ then $(\mathfrak{a} : x) = A$.

Proposition 9.7. *Let $\mathfrak{q} \subseteq A$ be $\mathfrak{p}$-primary.*

(1) If $x \notin \mathfrak{q}$, then $(\mathfrak{q} : x)$ is $\mathfrak{p}$-primary.

(2) If $x \notin \mathfrak{p}$, then $(\mathfrak{q} : x) = \mathfrak{q}$.

Proof. (1) Let $y \in (\mathfrak{q} : x)$. Then $xy \in \mathfrak{q}$, and so $y \in r(\mathfrak{q}) = \mathfrak{p}$. This shows that $\mathfrak{q} \subseteq (\mathfrak{q} : x) \subseteq \mathfrak{p}$, and when we apply r, we get $\mathfrak{p} = r(\mathfrak{q} : x)$. The only thing we need to check is that $(\mathfrak{q} : x)$ is primary.

Let $yz \in (\mathfrak{q} : x)$ with $y \notin (\mathfrak{q} : x)$. Then $xyz \in \mathfrak{q}$ and $xy \notin \mathfrak{q}$, and so $z^k \in \mathfrak{q}$ for some k. Then $z^k \in (\mathfrak{q} : x)$. This finishes the proof.

(2) Take an element $x \notin \mathfrak{p}$. Then $\overline{x}$ is not nilpotent in $A/\mathfrak{q}$. Since $\mathfrak{q}$ is $\mathfrak{p}$-primary, this implies that $\overline{x}$ is not a zero divisor in $A/\mathfrak{q}$. Therefore $xy \in \mathfrak{q}$ implies $y \in \mathfrak{q}$. □

9.2 Primary decomposition

Definition 9.8. Let $\mathfrak{a} \subseteq A$ be an ideal. A **primary decomposition** of a finite set $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_n\}$ of (distinct) primary ideals such that $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$. It is **minimal** if

[Min 1] the radicals are distinct,

[Min 2] $\mathfrak{q}_i \not\supseteq \bigcap_{j \neq i} \mathfrak{q}_j$ for all i.

If you have several that has the same radical, then you can collect them and replace by their intersection, which is again a primary ideal. This is the first minimality condition, and the second one only says to not use ideals that you don't need. We say that $\mathfrak{a}$ is **decomposable** if it has a primary ideal.

Proposition 9.9 (First uniqnuess theorem)**.** *Let $\mathfrak{a} \subseteq A$ be decomposable. Let $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_n\}$ be a primary decomposition. Suppose it is minimal, and let $\mathfrak{p}_i = r(\mathfrak{q}_i)$. Then the primes in the set $\{r(\mathfrak{a} : x) : x \in A\}$ are exactly the $\mathfrak{p}_i$. Thus n and $\{\mathfrak{p}_i\}_{i=1}^n$ are unique for $\mathfrak{a}$.*

Proof. We remark that for all $x \in A$,

$$(\mathfrak{a} : x) = \left(\bigcap_{i=1}^n \mathfrak{q}_i : x\right) = \bigcap_{i=1}^n (\mathfrak{q}_i : x) = \bigcap_{x \notin \mathfrak{q}_i} (\mathfrak{q}_i : x).$$

So $r(\mathfrak{a} : x) = \bigcup_{x \notin \mathfrak{q}_i} \mathfrak{p}_i$.

Let $x \in A$ such that $(\mathfrak{a} : x)$ is prime. Then $(\mathfrak{a} : x) = \bigcap_{x \notin \mathfrak{q}_i} \mathfrak{p}_i$. Then there exists an i_0 such that $(\mathfrak{a} : x) = \mathfrak{p}_i$ because $(\mathfrak{a} : x)$ is prime.

Now consider any $i_0 \in \{1, \ldots, n\}$. By [Min 2], there exists an $x_0 \notin \mathfrak{q}_{i_0}$ such that $x_0 \in \bigcap_{i \neq i_0} q_i$. Then

$$r(\mathfrak{a} : x_0) = \bigcap_{x_0 \notin \mathfrak{q}_i} \mathfrak{p}_i = \mathfrak{p}_{i_0}. \qquad \square$$

10 September 23, 2016

10.1 Associated primes

Definition 10.1. The **associated primes** of $\mathfrak{a}$ is

$$\mathrm{AP}(\mathfrak{a}) = \{\text{all primes of the form } (\mathfrak{a} : x) \text{ for } x \in A\}.$$

Even if $\mathfrak{a}$ is not decomposable, associated primes always exists. What we have proved is that if $\mathfrak{a}$ is decomposition, this is exactly those appearing in the decomposition. In the non-noetherian case, this can easily be infinite.

Definition 10.2. Let $\mathfrak{p}$ be an associate prime. We say that $\mathfrak{p}$ is **isolated** if it is minimal in $\mathrm{AP}(\mathfrak{a})$. The prime $\mathfrak{p}$ is embedded otherwise.

Proposition 10.3. *Let $\mathfrak{a} \subseteq A$ be decomposable. Every $\mathfrak{p} \supseteq \mathfrak{a}$ prime also contains some element of $\mathrm{AP}(\mathfrak{a})$.*

Proof. Let $p \supseteq \mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ be a minimal primary decomposition. Taking the radical, we get

$$\mathfrak{p} \supseteq \bigcap_{i=1}^{n} \mathfrak{p}_i.$$

Because $\mathfrak{p}$ is prime, $\mathfrak{p} \supseteq \mathfrak{p}_{i_0}$ for some i_0. □

Corollary 10.4. *The isolated primes of a decomposable ideal $\mathfrak{a}$ are exactly the minimal $\mathfrak{p}$ containing $\mathfrak{a}$.*

Localization is useful because you can throw away some primes and select primes you want. Taking the quotient throws away things that are below, but taking the localization throws way primes that are above. Because minimal primes are the good primes, localization is what you want to do.

Proposition 10.5. *Let $S \subseteq A$ be a multiplicative set, and let $\mathfrak{q}$ be an $\mathfrak{p}$-primary ideal.*

(1) $S \cap \mathfrak{p} \neq \emptyset$ implies $S^{-1}\mathfrak{q} = S^{-1}A$.

(2) $S \cap \mathfrak{p} = \emptyset$ implies that $S^{-1}\mathfrak{q}$ is $S^{-1}\mathfrak{p}$-primary and $\mathfrak{q} = \lambda_S^{-1}((\lambda_S(\mathfrak{q}))$.

Proof. (1) If $t \in S \cap \mathfrak{p}$ then there exists n with $t^n \in S \cap \mathfrak{q}$.

(2) Assume $S \cap \mathfrak{p} = \emptyset$. We remark that if $t \in S$ and $xt \in \mathfrak{q}$ then $x \in \mathfrak{q}$ or $t^n \in \mathfrak{q}$. But the second is not possible because $S \cap \mathfrak{p} = \emptyset$. So $x \in \mathfrak{q}$.

Clearly $\lambda^{-1}(S{-}1\mathfrak{q}) \subset \mathfrak{q}$ set-theoretically. Let $x \in \lambda^{-1}(S^{-1}\mathfrak{q})$. Then $x/1 = y/t$ for some $y \in \mathfrak{q}$ and $t \in S$. Then there exists $r \in S$ such that $rtx = ry \in \mathfrak{q}$. Then by the remark, $x \in \mathfrak{q}$. This shows that $\lambda_S^{-1}(S^{-1}\mathfrak{q})$.

Finally

$$r(S^{-1}\mathfrak{q}) = S^{-1}(r(f)) = S^{-1}p.$$

You can check that $S^{-1}\mathfrak{q}$ is primary using the isomorphism $S^{-1}A/S^{-1}\mathfrak{q} \cong \bar{S}^{-1}(A/\mathfrak{q})$. □

Definition 10.6. The **saturation** by S of an ideal $\mathfrak{a} \subseteq A$ is

$$S(\mathfrak{a}) = (\mathfrak{a}^e)^c = \lambda_S^{-1}((\lambda_S(\mathfrak{a})).$$

Proposition 10.7. *Let $S \subseteq A$ be a multiplicative set and suppose the ideal $\mathfrak{a} \subseteq A$ is decomposable. Let $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_n\}$ be a minimal decomposition with $\mathfrak{p}_i = r(\mathfrak{q}_i)$. Index the $\mathfrak{q}_i$'s su that $S \cap \mathfrak{p}_i = \emptyset$ for $i \leq m$ and $S \cap \mathfrak{p}_i \neq \emptyset$ for $i > m$. Then*

$$S^{-1}\mathfrak{a} = \bigcap_{i=1}^{m} S^{-1}\mathfrak{q}_i, \qquad S(\mathfrak{a}) = \bigcap_{i=1}^{m} \mathfrak{q}_i,$$

and the terms appearing are minimal primary decompositions.

Proof. This follows from the previous propositions. □

10.2 Second uniqueness of primary decomposition

Definition 10.8. A subset $\Sigma \subseteq \mathrm{AP}(\mathfrak{a})$ is **isolated** if given any $\mathfrak{p}' \in \mathrm{AP}(\mathfrak{a})$, $\mathfrak{p} \in \Sigma$, if $\mathfrak{p} \supseteq \mathfrak{p}'$ then $\mathfrak{p}' \in \Sigma$.

For example, $\Sigma = \mathrm{AP}(\mathfrak{a})$ is isolated, $\Sigma = \{\mathfrak{p}\}$ is isolated for isolated $\mathfrak{p}$.

Proposition 10.9 (Second uniqueness theorem)**.** *Let $\mathfrak{a} \subseteq A$ be decomposable and $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_n\}$ be a minimal primary decomposition. Let $\Sigma = \{\mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_k}\}$ is an isolated set for $\mathfrak{p}_i = r(\mathfrak{q}_i)$. Then $\bigcap_{j=1}^{k} \mathfrak{q}_{i_j}$ only depends on $\mathfrak{a}$ and Σ, not on the primary decomposition.*

Proof. Let $S_\Sigma = A \setminus \bigcup_{\mathfrak{p} \in \Sigma} \mathfrak{p}$, which is multiplicatively closed. Let $\mathfrak{p} \in \mathrm{AP}(\mathfrak{a})$. There are two cases. If $\mathfrak{p} \in \Sigma$, then $\mathfrak{p} \cap S_\Sigma = \emptyset$. If $\mathfrak{p} \notin \Sigma$, then $\mathfrak{p} \cap S_\Sigma \neq$. This is because the prime avoidance lemma tells us that $\mathfrak{p} \subseteq \bigcup_{i=1}^{k} \mathfrak{p}_{i_j}$ since Σ is isolated. Proposition 10.7 tells us that

$$\bigcap_{j=1}^{k} \mathfrak{q}_{i_j} = S_\Sigma(\mathfrak{a}),$$

which is independent of $\mathfrak{q}$. □

Corollary 10.10. *Let $\mathfrak{a}$ be a decomposition. The isolated components of a minimal decomposition of $\mathfrak{a}$ are unique.*

Example 10.11. Let $A = k[x, y]$ and let $\mathfrak{a} = (x^2, xy)$. You can write it as $\mathfrak{a} = (x) \cap (x, y)^2 = (x) \cap (x^2, y)$. In both cases, the associated primes are (x) and (x, y), with the first one isolated and the second one embedded. The isolated prime is determined as (x).

11 September 26, 2016

Today we will discuss integral algebras.

11.1 Integral algebras

Definition 11.1. Let $A \to B$ be an algebra. We say that $\beta \in B$ is **integral over** A if there is $f \in A[x]$ monic such that $f(\beta) = 0$. This f is called a **integrality relation**.

For example $\operatorname{im}(A \to B)$ has only integral elements. Also $\sqrt{2} \in \mathbb{C}$ is integral over $\mathbb{Z}$, with integrality relation $x^2 - 2$.

Proposition 11.2. *The following are equivalent:*

(1) $\beta \in B$ is integral over A.

(2) $A[\beta] \leq B$ is finitely generated as an A-module.

(3) There exists a subring $C \leq B$ containing $A[\beta]$ that is finitely generated as an A-module.

(4) There exists a $A[\beta]$-module M that is faithful (i.e. $\operatorname{Ann}_{A[\beta]} M = 0$) and finitely generated as an A-module.

Proof. For (1) $\Rightarrow$ (2), let f be an integral relation for β, with $\deg f = n \geq 1$. Then

$$\beta^n = -\alpha_{n-1}\beta^{n-1} - \cdots - \alpha_1\beta - \alpha_0.$$

Then $A[\beta] = \langle 1, \beta, \ldots, \beta^{n-1} \rangle$.

For (2) $\Rightarrow$ (3), take $C = A[\beta]$.

For (3) $\Rightarrow$ (4), take $M = C$. This is faithful because $1 \in C$.

For (4) $\Rightarrow$ (1), use Cayley-Hamilton with $\mathfrak{a} = A$ and endomorphism $\mu_\beta : M \to M$, $v \mapsto \beta v$. Then the relation is monic. □

Corollary 11.3. *Let $\beta_1, \ldots, \beta_r \in B$ be integral over A. Then $A[\beta_1, \ldots, \beta_r]$ is a finitely generated A-module.*

Proof. Induct on r. □

For C an A-algebra, we say that

(1) C is a **finite** A-algebra if C is finitely generated as an A-module,

(2) C is an A-algebra of **finite type** if C is finitely generated as an A-algebra, and

(3) C is **integral** over A if for any $\gamma \in C$, γ is integral over A.

Clearly (1) implies (2), and (2) does not imply (1). By the previous corollary, (2) and (3) imply (1).

Proposition 11.4. *Let B be an A-algebra, and let $\tilde{A} \subseteq B$ be the set of $\beta \in B$ that is integral over A. Then $\tilde{A}$ is a sub A-algebra of B.*

Proof. The only think we need to check is that $\tilde{A}$ is a ring (with operations and 1 of B). Let $\alpha, \beta \in \tilde{A}$. The rings $A[\alpha+\beta]$ and $A[\alpha-\beta]$ and $A[\alpha\beta]$ are all subrings of $A[\alpha, \beta]$. Since $A[\alpha, \beta]$ is finitely generated as an A-module, Proposition 11.2 (3) $\Rightarrow$ (1) shows that $\alpha + \beta$, $\alpha - \beta$, and $\alpha\beta$ are all integral over A. □

Definition 11.5. We call $\tilde{A}$ the **integral closure** of A in B. (Note that $A \not\subseteq \tilde{A}$ in general.)

Proposition 11.6. *Let $\varphi : A \to B$ and $\psi : B \to C$ be morphisms. If φ and ψ are integral, then $\psi \circ \varphi$ is integral.*

Proof. Exercise. □

Corollary 11.7. *If B is an A-algebra, then $\tilde{\tilde{A}} = \tilde{A}$.*

Proof. By definition of the integral closure, both maps

$$A \longrightarrow \tilde{A} \longrightarrow \tilde{\tilde{A}}$$

are integral, and so the composition is also integral. Then $\tilde{\tilde{A}} \subseteq \tilde{A}$, but we clearly have the other inclusion. □

Proposition 11.8. *Let $\varphi : A \to B$ be integral.*

(1) Given $\mathfrak{b} \subseteq B$ an ideal, let $\mathfrak{a} = \varphi^{-1}(\mathfrak{b})$. Then $\bar{\varphi} : A/\mathfrak{a} \to B/\mathfrak{b}$ is integral.

(2) Given $S \subseteq A$ a multiplicative set, $S^{-1}\varphi : S^{-1}A \to S^{-1}B$ is integral.

Proof. (1) Use the same integrality relations and reduce modulo the ideals.

(2) Let $\beta/t \in S^{-1}B$. Let $f(x) = x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_0$ be an integrality relation for β over A. Then

$$g(x) = x^n + \frac{\alpha_{n-1}}{t}x^{n-1} + \cdots + \frac{\alpha_0}{t^n} \in (S^{-1}A)[x]$$

is an integrality relation for β/t. □

11.2 Notion of a scheme

Last time we started with a ring A and set $X = \operatorname{Spec} A = \{\mathfrak{p} \subseteq A \text{ prime}\}$. Our goal was to do geometry on X, think of A as functions on X, and think of A-modules sheaves on X.

In the assignment, you will define the **Zariski topology** on X. For $\alpha \subseteq A$ an ideal, we define

$$V(\mathfrak{a}) = \{p \in X : p \supseteq \mathfrak{a}\}.$$

As $\mathfrak{a}$ varies, $V(\mathfrak{a})$ are the closed sets for this topology.

The functions are not really functions in the sense that each point has a value in different target spaces. Given $f \in A$, given $f \in A$ and $\mathfrak{p} \in X$, define:

(1) the residue of field at $\mathfrak{p}$ which is $k_{\mathfrak{p}} = A_{\mathfrak{p}}/\mathfrak{p}$,
(2) the value of f at $\mathfrak{p}$ is $f(\mathfrak{p}) = \bar{f} \in k_{\mathfrak{p}}$.

In particular, you have the notion of a zero set of f. Let

$$Z(f) = \{\mathfrak{p} \in X : f(\mathfrak{p}) = 0\} = \{\mathfrak{p} \in X : f \in \mathfrak{p}\}.$$

This is just $V((f))$ so it is closed.

12 September 28, 2016

Today we will discuss the Going-up theorem. We are going to consider $A \subseteq B$ that are integral, and study how prime ideals in A control primes in B.

12.1 Going-up theorem

Proposition 12.1. *Let $A \subseteq B$ be integral with A and B integral domains. Then A is a field if and only if B is a field (i.e., 0 is maximal in A if and only if 0 is maximal in B).*

Proof. We show the forward direction first. Assume that A is a field. Let $0 \neq \beta \in B$, and we want to show that β is invertible. Let $\beta^m + \alpha_{n-1}\beta^{n-1} + \cdots + \alpha_0 = 0$ be an integrality relation of minimal degree. Note that $\alpha_0 \neq 0$. Otherwise $\beta(\beta^{n-1} + \alpha_{n-1}\beta^{n-2} + \cdot + \alpha_1) = 0$ and B is an integral domain, so we get an integrality relation of degree $n-1$. Then we can rewrite the integrality relation with $\alpha_0 = -1$, because A is a field. Then you end up with

$$\alpha_n\beta^n + \alpha_{n-1}\beta^{n-1} + \cdots + \alpha_1\beta = 1.$$

Factoring β, we see $\beta(\alpha_n\beta^{n-1} + \cdots + \alpha_1) = 1$, that is, $\beta \in B^\times$.

Now let us assume that B is a field and let $0 \neq \alpha \in A$. Consider α^{-1}, which exists in B. By integrality, there exist $\gamma_i \in A$ such that

$$\alpha^{-n} + \gamma_{n-1}\alpha^{1-n} + \cdots + \gamma_1\alpha^{-1} + \gamma_0 = 0.$$

Then $\alpha^{-1} = -\gamma_{n-1} - \gamma_{n-2}\alpha - \cdots - \gamma_0\alpha^{n-1} \in A$. □

Corollary 12.2. *Let $A \subseteq B$ be integral, and let $\mathfrak{q} \subseteq B$ be prime with $\mathfrak{p} = \mathfrak{q}^c = \mathfrak{q} \cap A$. (Then $\mathfrak{p}$ is prime.) We have that $\mathfrak{q}$ is maximal in B if and only if $\mathfrak{p}$ is maximal in A.*

Proof. We made a remark last time that integrality is preserved under taking quotients. □

Proposition 12.3 ("Uniqueness")**.** *Let $A \subseteq B$ be integral. Let $\mathfrak{q} \subseteq \mathfrak{q}' \subseteq B$ be primes. Suppose that $\mathfrak{q}^c = \mathfrak{q}'^c$ in A. Then $\mathfrak{q} = \mathfrak{q}'$.*

Proof. Let $\mathfrak{p} = \mathfrak{q}^c = (\mathfrak{q}')^c \subseteq A$, which is a prime. Let $S = A \setminus \mathfrak{p}$. Then $A_\mathfrak{p} = S^{-1}A \subseteq S^{-1}B = B_\mathfrak{p}$ is integral. Let $\mathfrak{m} = \mathfrak{p}^e \subseteq A_\mathfrak{p}$ be the only maximal ideal in $A_\mathfrak{p}$, as $A_\mathfrak{p}$ is a local ring. Let $\mathfrak{n}, \mathfrak{n}' \subseteq B_\mathfrak{p}$ be the extensions of $\mathfrak{q}$ and $\mathfrak{q}'$. Clearly $\mathfrak{n} \subseteq \mathfrak{n}'$, and they are primes because S does not intersect $\mathfrak{q}$ and $\mathfrak{q}'$. Note that both $\mathfrak{n}$ and $\mathfrak{n}'$ contract to $\mathfrak{m}$ in $A_\mathfrak{p}$. So both $\mathfrak{n}$ and $\mathfrak{n}'$ are maximal in $B_\mathfrak{p}$, with $\mathfrak{n} \subseteq \mathfrak{n}'$. Therefore $\mathfrak{n} = \mathfrak{n}'$. Since localization gives a bijection on (suitable) primes, we get $\mathfrak{q} = \mathfrak{q}'$. □

Proposition 12.4 (Existence)**.** *Let $A \subseteq B$ be integral, and let $\mathfrak{p} \subseteq A$ be prime. Then there is a prime $\mathfrak{q} \subseteq B$ such that $\mathfrak{p} = \mathfrak{q}^c$ $(= \mathfrak{q} \cap A)$.*

Proof. We have a diagram

$$\begin{array}{ccc} A & \xhookrightarrow[\text{integral}]{i} & B \\ \downarrow{\scriptstyle \lambda} & & \downarrow{\scriptstyle \lambda'} \\ A_{\mathfrak{p}} & \xhookrightarrow[\text{integral}]{i_{\mathfrak{p}}=S^{-1}i} & B_{\mathfrak{p}} = S^{-1}B \end{array}$$

The prime $\mathfrak{p}$ extends to the maximal ideal $\mathfrak{m} = \mathfrak{p}^e$, and $\mathfrak{p} = \mathfrak{m}^c$. Now take any $\mathfrak{n} \subseteq B_{\mathfrak{p}}$ that is maximal. By the corollary, $\mathfrak{n}^c$ is maximal in $\mathfrak{A}_{\mathfrak{p}}$, and because $i_{\mathfrak{p}}$ is integral and $\mathfrak{A}_{\mathfrak{p}}$ is maximal, we have $\mathfrak{n}^c = \mathfrak{m}$. Now take $\mathfrak{q} = \lambda'^{-1}(\mathfrak{n}) \subseteq B$. Clearly $\mathfrak{q}$ is prime, and

$$i^{-1}(\mathfrak{q}) = i^{-1}(\lambda'^{-1}(\mathfrak{n})) = \lambda^{-1}(i_{\mathfrak{p}}^{-1}(\mathfrak{n})) = \lambda^{-1}(\mathfrak{m}) = \mathfrak{p}.$$

□

Theorem 12.5 (Going-up theorem)**.** *Let $A \subseteq B$ be integral. Let $\mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ be primes in A. Let $k < n$ and let $\mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_k$ be primes in B such that $\mathfrak{p}_i = \mathfrak{q}_i^c$ for $i \leq k$. Then there exist $\mathfrak{q}_j$ primes in B with $k < j \leq n$ such that*

$$\mathfrak{q}_1 \subsetneq \mathfrak{q}_2 \subsetneq \cdots \subsetneq \mathfrak{q}_k \subsetneq \cdots \subsetneq \mathfrak{q}_n$$

and $\mathfrak{p}_i = \mathfrak{q}_i^c$ for all $i = 1, \ldots, n$.

Proof. We turn $\subseteq$ to $\subsetneq$ by Proposition 12.3. For $k = 0$, we get $\mathfrak{q}_1$ by Proposition 12.4. Then quotient by $\mathfrak{q}_1$ and get $\mathfrak{q}_2$, and so on. □

12.2 Geometric interlude: Morphisms

There is a topology on schemes, as I have said. Let $X = \operatorname{Spec} A$ and $Y = \operatorname{Spec} B$. For any ring morphism $\phi : A \to B$ a morphism of rings, there is a set-theoretical map

$$\psi : Y \to X; \quad \mathfrak{p} \mapsto \psi(\mathfrak{p}) = \phi^{-1}(\mathfrak{p}).$$

An exercise is that ψ is continuous.

This gives a notion of pullback of functions. If $f \in A$ is a function on X, then we can define the pullback as $\psi^* f = \phi(f) \in B$ as a function on Y. To go further, we need the notion of sheaves. I leave it as an assignment to study the definition of a sheaf of abelian groups on a topological space.

13 September 30, 2016

Today we are going to discuss the going down theorem. Recall that the going up theorem told us the existence of an extension of a chain upstairs $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_k$. The going down theorem will tell us the existence of an extension in the other direction $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_k$.

The reason we call A downstairs and B upstairs in $A \to B$ is psychological. In the corresponding map of Specs, the direction of the arrows are reversed and we are lifting points.

13.1 Going down theorem

Lemma 13.1. *Let $f : A_1 \to A_2$ be a morphism of rings. Let $\mathfrak{p} \subseteq A_1$ be prime. Then there exists a prime $\mathfrak{q} \subseteq A_2$ with $\mathfrak{p} = \mathfrak{q}^c$ if and only if $\mathfrak{p} = \mathfrak{p}^{ec}$.*

Note that $\mathfrak{p}^e$ has no reason to be prime.

Lemma 13.2. *Let $A \subseteq B$ be integral domains and let $S \subseteq A$ be a multiplicative set. Then $S^{-1}\tilde{A} = \widetilde{S^{-1}A}$ in $S^{-1}B$.*

Definition 13.3. Let A be an integral domain. We say that A is **integrally closed** if $A = \tilde{A}$ in $K = \mathrm{Quot}(A) = (A \setminus \{0\})^{-1}A$.

For example, $\mathbb{Z}$, $\mathbb{Z}[\sqrt{-1}]$, $k[x]$ are all integrally closed. In fact, if A is a UFD then A is integrally closed.

Proposition 13.4. *Let A be an integral domain. Then the following are equivalent:*

(1) A is integrally closed.

(2) $A_{\mathfrak{p}}$ is integrally closed for all prime $\mathfrak{p} \subseteq A$.

(3) $A_{\mathfrak{m}}$ is integrally closed for all maximal $\mathfrak{m} \subseteq A$.

Proof. (1) $\Rightarrow$ (2) follows from Lemma 13.2. (2) $\Rightarrow$ (3) is trivial. For (3) $\Rightarrow$ (1), consider $\tilde{A} \subseteq K = \mathrm{Quot}\, A$. Let $f : A \to \tilde{A}$. This map in injective because $A \subseteq K$. Also f is surjective because surjectivity is local. Thus $A = \tilde{A}$. □

Let $A \subseteq B$ be rings and $\mathfrak{a} \subseteq A$ be an ideal, and $\beta \in B$. We say that β is **integral over** $\mathfrak{a}$ if there exist $\alpha_j \in \mathfrak{a}$ such that

$$\beta^n + \alpha_{n-1}\beta^{n-1} + \cdots + \alpha_0 = 0.$$

Lemma 13.5. *If $A \subseteq B$ are rings and $\mathfrak{a} \subseteq B$ are ideals, then $\tilde{\mathfrak{a}} = r_{\tilde{A}}(\mathfrak{a}\tilde{A}) \subseteq B$ (which has no reason to be an ideal of B). So it is closed under addition and multiplication.*

Proof. Let us first prove $\subseteq$. Let $\beta \in \tilde{\mathfrak{a}} \subseteq \tilde{A}$. Now

$$\beta^n = -\alpha_{n-1}\beta^{n-1} - \cdots - \alpha_0 \in \mathfrak{a}\tilde{A}.$$

This shows that $\beta \in r_{\tilde{A}}(\mathfrak{a}\tilde{A})$.

For $\supseteq$, let $\beta \in r_{\tilde{A}}(\mathfrak{a}\tilde{A})$. Then there exists some n with $\beta^n \in \mathfrak{a}\tilde{A}$. Then

$$\beta^n = \alpha_1\gamma_1 + \cdots + \alpha_r\gamma_r$$

with $\alpha_j \in \mathfrak{a}$ and $\gamma_j \in \tilde{A}$. Now consider $M = A[\gamma_1, \ldots, \gamma_r]$, which is finitely generated over A because γ_j are integral. Because $\beta^n M \subseteq \mathfrak{a}M$, we can apply Nakayama and see that $\beta^n \in \tilde{\mathfrak{a}}$. It follows that $\beta \in \tilde{\mathfrak{a}}$. □

Proposition 13.6. *Let $A \subseteq B$ be integral domains with A integrally closed (inside its fractional field). Let $\mathfrak{a} \subseteq A$ be an ideal and $\beta \in \tilde{a}$ ($\subseteq B$) and $K = \mathrm{Quot}(A)$. Then β is algebraic over K and its minimal polynomial over K has the form*

$$f(x) = x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_0 \in K[x]$$

with $\alpha_j \in r_A(\mathfrak{a})$.

Proof. Let L/K be the splitting field of f over K. Then all roots of f in L are integral over $\mathfrak{a}$, because all roots of f are the also roots of any polynomial having β as a root. Since $\tilde{\mathfrak{a}}$ is closed under addition and multiplication, $\alpha_j \in \tilde{\mathfrak{a}}$ for all j. Because A is integrally closed, $\mathfrak{a} = r_A(\mathfrak{a}A) = r_A(\mathfrak{a})$. □

For example, take $A = \mathbb{Z}$ and $B = \mathbb{Z}[i]$. Let $\mathfrak{a} = (4) \subseteq A$. Then A is integrally closed and $K = \mathbb{Q}$. Take $\beta = 1 + i \in \mathfrak{a}$ because $\beta^4 + 4 = 0$. The minimal polynomial is $f(x) - 2x + 2$ whose coefficients are in $(2) = r_A((4))$.

Theorem 13.7 (Going down theorem)**.** *Let $A \subseteq B$ be integral domains with $A \subseteq B$ integral and A integrally closed. Let $\mathfrak{p}_1 \supseteq \cdots \supseteq \mathfrak{p}_n$ be primes in A. Let $\mathfrak{q}_1 \supseteq \cdots \supset \mathfrak{q}_k$ ($k < n$) be primes in B with $\mathfrak{p}_i = \mathfrak{q}_i^c$ ($= \mathfrak{q} \cap A$). Then there exists $\mathfrak{q}_j \subseteq B$ primes such that $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_n$ and $\mathfrak{p}_i = \mathfrak{q}_i^c$.*

Proof. The case $k = 0$ and $n = 1$ is the same as the going up theorem. The general case follows from $k = 1$ and $n = 2$. It is enough to show $\mathfrak{p}_2 B_{\mathfrak{q}_1} \cap A = \mathfrak{p}_2$, by Lemma 13.1. We need to show $\mathfrak{p}_1 B_{\mathfrak{q}_1} \subseteq \mathfrak{p}_2$ because the other direction is trivial. Suppose $x \in \mathfrak{p}_2 B_{\mathfrak{q}_1} \cap A \setminus \mathfrak{p}_2$. Then $x \in \mathfrak{p}_2 B_{\mathfrak{q}_1}$ implies $x = y/s$ for some $x \in \mathfrak{p}_2 B$ and $s \in B \setminus \mathfrak{q}_1$. In this case, $y \in \mathfrak{p}_2 B \subseteq r_B(\mathfrak{p}_2 B) = \tilde{\mathfrak{p}}_2$ by Lemma 13.5. Then the minimal equation of y over K is

$$y^r + u_{r-1}y^{r-1} + \cdots + u_0 = 0$$

with $u_i \in r_A(\mathfrak{p}_2) = \mathfrak{p}_2$. Because $s = y \cdot x^{-1}$, with $x^{-1} \in K$ since $x \in A$, the minimal equation for s over K is

$$s^r + v_{r-1}s^{r-1} + \cdots + v_0 = 0$$

for $v_i = u_i/x^{r-i} \in K$. Hence $v_i \cdot x^{r-i} = u_i \in \mathfrak{p}_2$. On the other hand, since $s \in B$¡ it is integral over A. This shows that by Proposition 13.6, $v_i \in r_A(1 \cdot A) = A$. Since $v_i \cdot x^{r-i} = u_i \in \mathfrak{p}_2$ and $x \notin \mathfrak{p}_2$, $v_i \in \mathfrak{p}$. But then $s^r \in \mathfrak{p}_2 B \subseteq \mathfrak{p}_1 B \subseteq \mathfrak{q}_1$. This contradicts $B \setminus \mathfrak{q}_1$. □

14 October 3, 2016

Today we will study some connection between classical algebraic geometry and commutative algebra. Today, k is a field.

14.1 Noether normalization and Nullstellensatz

Lemma 14.1. *Let $x_1, \dots, x_r, z$ be variables, and let $f \in k[x][z]$ be non-constant in z. There are $\alpha \in k^\times$ and $N \geq 1$ such that*

$$F = \alpha \cdot f(x_1 + z^{N^1}, \dots, x_r + z^{N^r}, z)$$

is monic in z.

Proof. $N > \deg f$ works. □

Theorem 14.2 (Noether normalization lemma)**.** *Let $A \neq 0$ be a finitely generated k-algebra. There exist $x_1, \dots, x_r \in A$ algebraically independent over k such that $k[x_1, \dots, x_r] \subseteq A$ is integral.*

Proof. Let $x_1, \dots, x_n$ be generators for A as a k-algebra, indexed such that $x_1, \dots, x_r$ are algebraically independent over k and all x_i are algebraic over $k[x_1, \dots, x_r]$.

If $n = r$ then we are done. Suppose that $r < n$ and the result holds for any k-algebra with at most $n-1$ generators, by using induction on the number of generators.

Now because x_n is algebraic over $k[x_1, \dots, x_r]$, there exists a polynomial $f \in k[x_1, \dots, x_r][z]$ such that $f(x_1, \dots, x_r; x_n) = 0$ in A. By the previous lemma, $F = f(x_1 + z^{N^1}, \dots, x_r + z^{N^r}; z)$ monic in z. Define $y_i = x_i - x_n^{N^i}$ for $i \leq r$. Then $y_i \in A$, and $\tilde{F} = f(y_1 + z^{N^1}, \dots, y_r + z^{N^r}; z)$ is monic in z. Also $\tilde{F}(x_n) = 0$. This shows that x_n is integral over $k[y_1, \dots, y_r, x_{r+1}, \dots, x_{n-1}] \subseteq A$ but $k[y_1, \dots, y_r]$ is an k-algebra with at most $n-1$ generators, and hence integral over some polynomial ring. Because the composition integral extensions is an integral extension, we are done. □

The geometric interpretation is that any variety is integral over some affine space.

Lemma 14.3 (Zariski's lemma)**.** *Let L be a finitely generated k-algebra and suppose that L is a field. Then L/k is a finite algebraic extension. j*

Proof. Let L/k be a finitely generated k-algebra with L a field. Suppose L/k is not finite algebraic. Then Noether normalization implies that $k[\underline{x}] \subseteq L$ is integral for some algebraically independent $\underline{x}$. Because it is not finitely algebraic, $\underline{x} \neq \emptyset$. The ring $k[\underline{x}]$ has at least the ideals (0) and (x_1) with $(0) \subsetneq (x_1)$. Then going-up implies that L has at least 2 distinct prime ideals, which contradicts that L is a field. □

Theorem 14.4 (Weak Nullstellensatz)**.** *Let k be algebraically closed. Let $n \geq 1$. Then the maximal ideals of $k[x_1, \ldots, x_n]$ are exactly of the form*

$$(x_1 - \alpha_1, \ldots, x_n - \alpha_n)$$

with $\alpha_j \in k$. Thus we have bijections

$$\left\{ \begin{matrix} \textit{maximal ideals of} \\ k[x_1, \ldots, x_n] \end{matrix} \right\} \quad \longleftrightarrow \quad \mathrm{Mor}_{k\text{-}Alg}(k[x_1, \ldots, x_r], k) \quad \longleftrightarrow \quad k^n.$$

Proof. Those ideals of that form are kernels of the maps $\phi_{(\alpha_i)} : k[\underline{x}] \to k$ given by $x_i \mapsto \alpha_i$.

Let $\mathfrak{m} \subseteq k[\underline{x}]$ be maximal. Then $L = k[\underline{x}]/\mathfrak{m}$ is a field, and Zariski's lemma tells us that L/k is a finite extension. Because k is algebraically closed, $k \hookrightarrow L$ is an isomorphism.

$$\begin{array}{ccc} k[\underline{x}] & \longrightarrow & L \\ & \searrow^{\phi_{\mathfrak{m}}} & \downarrow \cong \\ & & k \end{array}$$

Let $\phi_{\mathfrak{m}}(x_i) = \alpha_i$. Then $\phi_{\mathfrak{m}}(x_i - \alpha_i) = 0$ so $\mathfrak{m} \supseteq (x_1 - \alpha_1, \ldots, x_n - \alpha_n)$. Because $(x_1 - \alpha_1, \ldots, x_n - \alpha_n)$ is maximal, it follows that $\mathfrak{m}$ is exactly that ideal. $\square$

15 October 5, 2016

Theorem 15.1 (Weak Nullstellenstaz, High School version)**.** *Let k be an algebraically closed field with $n \geq 1$. Let $f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$. The following are equivalent:*

(1) $f_1, \ldots, f_r$ have no common zeros in k^n, i.e., the system $f_1 = 0, \ldots, f_r = 0$ has no solution in k^n.

(2) $(f_1, \ldots, f_r) = (1)$, i.e., there exist $g_1, \ldots, g_r \in k[\underline{x}]$ such that $g_1 f_1 + \cdots + g_r f_r = 1$.

Proof. (2) $\Rightarrow$ (1) is clear. Now we show (1) $\Rightarrow$ (2). Say (2) fails. Then there is a maximal $\mathfrak{m} \subseteq k[\underline{x}]$ such that $(f_1, \ldots, f_r) \subseteq \mathfrak{m}$. Then Nullstellensatz tell us that $\mathfrak{m} = (x_1 - \alpha_1, \ldots, x_n - \alpha_n)$. So $f_i = \sum_{j=1}^{n} h_{ij}(x_j - \alpha_j)$ for $h_{ij} \in k[\underline{x}]$. Then $(\alpha_1, \ldots, \alpha_n)$ is a common zero of all the f_i. □

Lefschetz's principle states that if you have a problem over an algebraically closed field of characteristic zero, then we may assume that we are working over $\mathbb{C}$. Let $f_1, \ldots, f_r \in \mathbb{Q}[\underline{x}]$, and let K be an algebraically closed field of characteristic 0. Suppose that they have a common zero in K^n. Then they have a common zero in $\overline{Q}$.

This is because if $f_1, \ldots, f_r$ has no common zero in $\overline{Q}^n$, then there are polynomials $g_1, \ldots, g_r \in \overline{Q}[x] \hookrightarrow K[x]$ such that $g_1 f_1 + \cdots + g_r f_r = 1$, because K is algebraically closed. Hence also in $K[\underline{x}]$, $g_1 f_1 + \cdots + g_r f_r = 1$. Then $f_1, \ldots, f_r$ has no common zero over K.

Here is another way of thinking about this. Say that the solution $(\alpha_j)_{j-1}^n$ is in $\alpha_j \in \overline{\mathbb{Q}}[\pi] \subseteq \mathbb{C}$ for simplicity. Then $\alpha_j \in \overline{\mathbb{Q}}[\pi] \cong \overline{\mathbb{Q}}[z] \subseteq \mathbb{C}$. Then we can specialize to $z = 0$ to get a solution in $\overline{\mathbb{Q}}$.

15.1 Chain conditions

Definition 15.2. Let A be a ring and M an A-module. We say that M satisfies:

(1) the **ascending chain condition** if given any chain $N_1 \leq N_2 \leq \cdots \leq M$, there exist and n such that $N_j = N_n$ for all $j \geq n$.

(2) the **descending chain codition** if given any $M \geq N_1 \geq \cdots$, there exists n such that $N_j = N_n$ for all $j \geq n$.

Definition 15.3. M is **Noetherian** if it satisfies the ascending chain condition. M is **Artinian** if it satisfies the descending chain condition. A ring A is P if it is P as an A-module, where P is "Noetherian" or "Artinian".

Proposition 15.4. *Let M be an A-module. Then the following are equivalent:*

(1) M is Noetherian.

(2) Every collection $\Sigma \neq \emptyset$ of submodules of M has a maximal element (in Σ).

(3) For all $N \leq M$, N is finitely generated.

Proof. (1) $\Rightarrow$ (2) is easy. For (2) $\Rightarrow$ (3), take $\Sigma = \{Q \leq N : Q \text{ is finitely generated}\}$. Let $Q_0 \in \Sigma$ be maximal. Then $Q_0 = N$, for otherwise $Q_1 = Q_0 + \langle x \rangle$ for $x \in N \setminus Q_0$ is finitely generated.

For (3) $\Rightarrow$ (1), take $N_1 \leq N_2 \leq \cdots \subseteq M$. Let $N = \bigcup_{j=1} N_j$. This is a submodule because it is a nested union. Then $N = \langle x_1, \ldots, x_r \rangle$ and once N_n contains $x_1, \ldots, x_r$ we will have $N_n = N$. □

Proposition 15.5. *Let X be "Noetherian" or "Artinian". We have:*

(1) If $0 \to M \to N \to P \to 0$ is exact, then N is X if and only if M and P are X.

(2) X is preserved by finite direct sums.

(3) X for A-modules is preserved by arbitrary quotients.

(4) If A is a X ring and M is a finitely generated A-module, then M is X.

Proof. First check (1). Then everything follows. □

Proposition 15.6. *Let A be a Noetherian ring and $S \subseteq A$ be a multiplicative set. This implies that $S^{-1}A$ is Noetherian.*

Proof. Every ideal of $S^{-1}A$ is of the form $\mathfrak{a}^e$ with $\mathfrak{a} \subseteq A$ an ideal. Then check finite generation. □

Next time we will do the Hilbert basis theorem.

16 October 7, 2016

Last time we introduced the notion of Noetherian modules and Noetherian rings.

16.1 Hilbert basis theorem

Theorem 16.1 (Hilbert basis theorem)**.** *If A is Noetherian and x is a variable then $A[x]$ is Noetherian.*

Corollary 16.2. *If k is a field, then $k[x_1, \dots, x_n]$ is Noetherian. Likewise, $\mathbb{Z}[x_1, \dots, x_n]$ is Noetherian.*

Corollary 16.3. *If k is a field, then k-algebras of finite type are Noetherian. Likewise finitely generated rings are Noetherian.*

Proof of Theorem 16.1. Let $\mathfrak{a} \subseteq A[x]$ be an ideal. Consider the set

$$\operatorname{lc}(\mathfrak{a}) = \{\text{leading coefficients of elements in } \mathfrak{a}\} \subseteq A.$$

This is clearly an ideal of $\mathfrak{a}$. Because A is Noetherian, $\operatorname{lc}(\mathfrak{a}) = (\alpha_1, \dots, \alpha_n)$.

Let $f_j \in \mathfrak{a}$ be such that

$$f_j = \alpha_j x^{d_j} + \text{lower degree terms},$$

and let $\mathfrak{a}' = (f_1, \dots, f_n) \subseteq A[x]$. Take any $f = \alpha x^m + (\text{lower degree terms})$. Then

$$\alpha = \sum_{j=1}^{n} \beta_j \alpha_j, \quad \beta_j \in A$$

because $\alpha \in \operatorname{lc}(\mathfrak{a})$.

Now we claim that there exists an $g \in \mathfrak{a}$ such that $\deg g < d = \max d_j$ with $f = g + h$ and $h \in \mathfrak{a}'$. If $m < d$, then we are done. Otherwise look at $f - \sum_{j=1}^{m} \beta_j f_j x^{m-d_j}$, which has smaller degree. Repeating this step, we get a decomposition of f into something in $\mathfrak{a}$ and small degree.

Finally let $M = \langle 1, x, \dots, x^{d-1} \rangle \subseteq A[x]$ as an A-module. Then $\mathfrak{a} = \mathfrak{a}' + (M \cap \mathfrak{a})$. Because A is Noetherian and M is finitely generated, M is a Noetherian module. Then $\mathfrak{a} \cap M$ is finitely generated. Thus $\mathfrak{a}$ is finitely generated. □

As an exercise, let k be a field and let x be a variable, and prove that $k[[x]]$ is Noetherian. There is an elementary proof, but a more conceptual way is to use that the property of being Noetherian is preserved under completion.

16.2 Irreducible ideals and primary decomposition

Definition 16.4. Let A be a ring. We say that an ideal $\mathfrak{a} \subseteq A$ is irreducible if $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ implies $\mathfrak{a} = \mathfrak{b}$ or $\mathfrak{a} = \mathfrak{c}$.

Lemma 16.5. *If A is Noetherian, then every ideal is a finite intersection of irreducible ideals.*

Proof. Otherwise there exists $\mathfrak{a} \subseteq A$ maximal among the ideals that are not finite intersections of irreducible ideals. Because $\mathfrak{a}$ is not maximal, there exist $\mathfrak{a} \subsetneq \mathfrak{b}$ and $\mathfrak{a} \subsetneq \mathfrak{c}$ such that $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$. Because $\mathfrak{a}$ is maximal, there exist ways to represent $\mathfrak{b}$ and $\mathfrak{c}$ as finite intersections of irreducible ideals. Then $\mathfrak{a}$ is an intersection of irreducible ideals. □

Lemma 16.6. *Let A be Noetherian and let $\mathfrak{a} \subsetneq A$ be an ideal. If $\mathfrak{a}$ is irreducible, then it is primary.*

Proof. We can assume that $\mathfrak{a} = (0)$ by looking at the quotient. Assume that (0) is irreducible. Let $x, y \in A$ with $xy = 0$ and $y \neq 0$. We want to show that x is nilpotent. By the ascending chain condition, there exists an n such that

$$\operatorname{Ann}(x^n) = \operatorname{Ann}(x^{n+1}) = \cdots .$$

Now we claim that $(x^n) \cap (y) = (0)$. Let $z \in (x^n) \cap (y)$. Then $zx = 0$ as $z \in (y)$. Also $z = \alpha x^n$ as $z \in (x^n)$. Then $0 = zx = \alpha x^{n+1}$, and then $\alpha \in \operatorname{Ann}(x^{n+1}) = \operatorname{Ann}(x^n)$. This implies that $0 = \alpha x^n = z$.

Now $(x^n) \cap (y) = 0$, which is irreducible. This implies that $x^n = 0$ or $y = 0$. □

Proposition 16.7. *Let A be Noetherian. Then every proper ideal of A has a primary decomposition.*

Lemma 16.8. *Let A be Noetherian, and let $\mathfrak{a} \subseteq A$ be an ideal. Then there exists an integer n such that $r(\mathfrak{a})^n \subseteq \mathfrak{a}$.*

Proof. $r(\mathfrak{a})$ is finitely generated, so $r(\mathfrak{a}) = (\alpha_1, \ldots, \alpha_k)$. Then $x \in r(\mathfrak{a})$ can be written as

$$x = \sum_{j=1}^{k} \beta_j \alpha_j.$$

Take $n > m_1 + \cdots + m_k$ where $\alpha_j^{m_j} \in \mathfrak{a}$. Then every term in the expansion of x^n has at least one of $\alpha_j^{m_j}$ in it, and so $x^n \in \mathfrak{a}$. Likewise any $x_1 \cdots x_n \in \mathfrak{a}$ for $x_1, \ldots, x_n \in r(\mathfrak{a})$. □

17 October 12, 2016

Today we are going to discuss Noetherian domains of dimension 1. Recall that if A is a ring, then the **Krull dimension** of A is maximal number proper inclusions of prime ideals in A. For example, $\dim \mathbb{Z} = 1$ because $\operatorname{Spec} \mathbb{Z} = \{(0)\} \cup \{(p) : \text{prime}\}$. Likewise $\operatorname{Spec} \mathbb{C}[x] = \{(0)\} \cup \{(x - \alpha) : \alpha \in \mathbb{C}\}$. In two variables,

$$\operatorname{Spec} \mathbb{C}[x, y] = \{(0)\} \cup \{(f) : f \text{ irreducible}\} \cup \{(x - \alpha, y - \beta) : \alpha, \beta \in \mathbb{C}\}.$$

As an exercise, prove that there are no other primes. So $\dim \mathbb{C}[x, y] = 2$. This easy description does not extend easily to more variables. Also as an exercise, describe $\operatorname{Spec} \mathbb{Z}[x]$. It also has dimension $\dim \mathbb{Z}[x] = 2$.

17.1 Discrete valuation rings

This is the local case for Noetherian domain of dimension 1.

Proposition 17.1. *Let A be a Noetherian domain with $\dim A = 1$. Every $\mathfrak{a} \subseteq A$ is the product of finitely many primary ideals with distinct radicals.*

Proof. Assume $\mathfrak{a} \neq (0)$. Because A is Noetherian, there exists a minimal primary decomposition

$$\mathfrak{a} = \bigcup_{i=1}^{n} \mathfrak{q}_i.$$

Let $\mathfrak{p}_i = r(\mathfrak{q}_i)$. Because $\dim A = 1$, all $\mathfrak{p}_i$ are maximal. That is, $\mathfrak{p}_i$ are pairwise coprime. Then

$$(1) = r((1)) = r(\mathfrak{p}_i + \mathfrak{p}_j) = r(r(\mathfrak{q}_i) + r(\mathfrak{q}_j)) = r(\mathfrak{q}_i + \mathfrak{q}_j).$$

So $\mathfrak{q}_i + \mathfrak{q}_j = (1)$. So the intersection is the same as the product. □

Definition 17.2. Let K be a field. A **discrete valuation** is a surjective map $v : K^\times \to \mathbb{Z}$ such that

(1) $v(xy) = v(x) + v(y)$,
(2) $v(x + y) \geq \min\{v(x), v(y)\}$.

So define $v(0) = +\infty$ and this is consistent with the previous conditions, giving $v : K \to \mathbb{Z} \cup \{+\infty\}$.

Example 17.3. For $K = \mathbb{Q}$ and a prime p, we have a valuation $v = v_p$ which is called the p-adic valuation. This is defined as

$$v_p\left(\frac{a}{b}\right) = n \text{ if } \frac{a}{b} = p^n \cdot \frac{a'}{b'}$$

with $(\mathfrak{a}', \mathfrak{b}') = 1$ and $p \nmid a', b'$.

Similarly, there is a valuation on $K = \mathbb{C}(x)$ for $\alpha \in \mathbb{C}[x]$, which is v_f, and another valuation $v = -\deg$.

Now define

$$\mathcal{O}_v = \{x \in K : v(x) \geq 0\}, \quad \mathfrak{m}_v = \{x \in K : v(x) > 0\}.$$

The $\mathcal{O}_v$ is called the **valuation ring of** v. It turns out that $(\mathcal{O}_v, \mathfrak{m}_v)$ is a local ring, and there is a residue field $k_v = \mathcal{O}_v/\mathfrak{m}_v$. For example, for $K = \mathbb{Q}$, we have $k_{v_p} = \mathbb{F}_p$.

Definition 17.4. An integral domain A is a **discrete valuation ring** if there exists a valuation v on $K = \mathrm{Quot}(A)$ such that $A = \mathcal{O}_v$.

From the previous examples, we see that $\mathbb{Z}_{(p)}$ and $\mathbb{C}[x]_{(x-\alpha)}$ are DVRs.

Proposition 17.5. *If A is a DVR, then*

(1) A is local,

(2) A is integrally closed,

(3) A is a PID,

(4) every nonzero ideal $\mathfrak{a} \subseteq A$ is a power of the maximal ideal,

(5) $\dim A = 1$,

(6) A is Noetherian,

(7) there exists $x \in A$ such that all nonzero ideals are (x^r) for $r \geq 0$.

Proof. (1) and (2) are clear. Say $v : K^\times \to \mathbb{Z}$ with $A = \mathcal{O}_v$ and $\mathfrak{m} = \mathfrak{m}_v$. Define the ideals

$$\mathfrak{m}_r = \{x \in K : v(x) \geq r\}.$$

Then $\mathfrak{m}_0 = A$, $\mathfrak{m}_1 = \mathfrak{m}$, and $\mathfrak{m}_i \supsetneq \mathfrak{m}_{i+1}$ because v is surjective. Let $\mathfrak{a} \subseteq A$ be a nonzero ideal. Take $r = \min\{v(x) : x \in \mathfrak{a}\}$ and take $x_r \in \mathfrak{a}$ with $v(x_r) = r$. For $y \in \mathfrak{a}$, $\mathfrak{y}/x_r \in \mathcal{O}_v$, and so $\mathfrak{a} \subseteq (x_r) \subseteq \mathfrak{a}$. That is, A is PID and $\mathfrak{a} = \mathfrak{m}_r$. For (7), we take $x \in \mathfrak{m}_1 \setminus \mathfrak{m}_2$. □

18 October 14, 2016

Last time we introduced the notion of a discrete valuation. Now I will explain why I call these Noetherian domains of dimension 1.

18.1 Local Noetherian domain of dimension 1

Proposition 18.1. *Let A be a local Noetherian domain of dimension 1, and let $\mathfrak{m}$ be the maximal ideal with $k = A/\mathfrak{m}$. The following are equivalent:*

(i) A *is a DVR.*

(ii) A *is integrally closed.*

(iii) $\mathfrak{m}$ *is principal.*

(iv) $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$.

(v) Every ideal $0 \neq \mathfrak{a} \subsetneq A$ *is a power of* $\mathfrak{m}$.

(vi) There is an element $x \in A$ *such that all ideals* $\mathfrak{a} \neq 0$ *are of the form* $\mathfrak{a} = (x^r)$ *for* $r = 0, 1, \ldots$.

The element x in (iv) is called the **uniformizer**. Heuristically, local Noetherian domains corresponds to neighborhoods of a singular point of a curve, and DVRs correspond to neighborhoods of smooth points of a curve. The process is taking the normalization $\tilde{A}$ of a local Noetherian domain A. For instance, take $A = \mathbb{Z}[\sqrt{5}]$ and $\tilde{A} = \mathbb{Z}[(1+\sqrt{5})/2]$. If we have a prime $p \subseteq A$ such that A_p is local Noetherian domain of dimension 1, but not a DVR. Then you can look at $\mathfrak{p} \subseteq \tilde{A}$ where $\mathfrak{p}^c = p$.

Proof. I'll just do the not-so-easy implications. Let us do (ii) $\Rightarrow$ (iii). Take $0 \neq x \in \mathfrak{m}$. We know that $(x) \subseteq \mathfrak{m}$, and so $r((x)) = \mathfrak{m}$. The Noetherian hypothesis tells us that there exists an t such that $\mathfrak{m}^t \subseteq (x)$ but $\mathfrak{m}^{t-1} \not\subseteq (x)$. Let $t \in \mathfrak{m}^{t-1} \setminus (x)$. Consider $z = x/y \in K = \operatorname{Quot}(A)$. Note that $z^{-1} \notin A$ because $y \notin (x)$. Then $z^{-1} \notin A = \tilde{A}$ because A is integrally closed, and it follows that $z^{-1}\mathfrak{m} \not\subseteq \mathfrak{m}$.

On the other hand, we claim that $z^{-1}\mathfrak{m} \subseteq A$. For any $\alpha \in \mathfrak{m}$,

$$\left(\frac{y}{x}\alpha\right)^t = \frac{y^t}{x^{t-1}}\frac{\alpha^t}{x} = \beta \in A$$

because $\alpha^t/x \in A$ since $\alpha^t \in \mathfrak{m}^t \subseteq (x)$ and $y^t \in \mathfrak{m}^{t(t-1)} \subseteq (x)^{t-1}$. Therefore $z^{-1}\alpha$ is a root of $X^t - \beta$, and thus $z^{-1}\alpha \in \tilde{A} = A$.

Now $z^{-1}\mathfrak{m}$ is an ideal of A, but it is not in $\mathfrak{m}$. Thus $z^{-1}\mathfrak{m} = A$. It follows that $\mathfrak{m} = zA = (z)$.

Another tricky implication is (iv) $\Rightarrow$ (v). Nakayama will imply that $\mathfrak{m}$ is principal, because you can lift the generator. Let t be the maximal exponent such that $\mathfrak{m}^t \supseteq \mathfrak{a}$, where $0 \neq \mathfrak{a} \subsetneq A$. Note that such a t exists because $\mathfrak{m}^n \subseteq \mathfrak{a}$ for some n by the Noetherian hypothesis, and then $\mathfrak{m}^{n+j} \subsetneq \mathfrak{a}$ for $j > 0$.

We want to show that there exists some $\alpha \in \mathfrak{a}$ such that $\alpha = x^t u$, where $u \in A^\times$. Otherwise, for all $\alpha \in \mathfrak{a}$ there exists an $u \in \mathfrak{m}$ such that $\alpha = x^t u$. Then $\alpha = x^{t+1} v$ for some $v \in A$. This shows that $\mathfrak{a} \subseteq \mathfrak{m}^{t+1}$, and we get a contradiction. Then $\mathfrak{m}^t \supseteq \mathfrak{a} \supseteq \mathfrak{m}^t$, i.e., $\mathfrak{a} = \mathfrak{m}^t$.

Finally let us prove (vi) $\Rightarrow$ (i). We need to construct a valuation $v : K^\times \to \mathbb{Z}$. For $\beta \in A$, define $v(\beta) = r_\beta$ where $(\beta) = (x^{r_\beta})$. Then you define

$$v\Big(\frac{\beta}{\gamma}\Big) = r_\beta - r_\gamma.$$

This is not a priori well-defined, but you can check that it is well-defined. □

Theorem 18.2. *Let A be a Noetherian domain of dimension 1. The following are equivalent:*

(1) A is integrally closed.

(2) Every primary ideal is a prime power.

(3) Every local ring $A_\mathfrak{p}$ (for $\mathfrak{p}$ maximal) is DVR.

Proof. Just localize at $\mathfrak{p}$ and use the previous theory. (Note that integrality is local.) □

Definition 18.3. Such a ring is called a **Dedekind domain**.

19 October 17, 2016

Last time we introduced Dedekind domains. A is a Dedekind domain if (1) A is Noetherian, (2) $\dim A = 1$, (3) any of the following equivalent condition holds:

(i) A is integrally closed.

(ii) Every primary ideal in A is a prime power.

(iii) Every local ring $A_{\mathfrak{p}}$ (with $\mathfrak{p}$ maximal) is a DVR.

Corollary 19.1. *If A is a Dedekind domain, then every nonzero ideal has a* unique *factorization as a product of powers of nonzero primes.*

There was an open problem of whether there is a solution to

$$x^n + y^n = z^n, \quad xyz \neq 0$$

for $n \geq 3$. Someone had this brilliant idea of writing it as

$$y^n = \prod_{\epsilon^n = 1} (z - \epsilon x).$$

If we have unique factorization or something similar, then it would follow that each term in the right hand side is a power because they are coprime. But this doesn't work if the ring is not a UFD. So Kronecker came up with the idea of working instead with the ideals. In this case, we have unique factorization. But some principal ideal being a nth power of some other ideal does not mean that it is a power of a principal ideal. If the ring is a PID, then we are good, but then there is no point in looking at the ideals. However, we only need some ideals being principal. If we allow some "inverse" of ideals, then the ideals form a group, and we can take the quotient by the subgroup of principal ideals. If this is a finite group, and has order coprime to n, then we are in business.

19.1 Fractional ideals

Let A be an integral domain, and let $K = \mathrm{Quot}(A)$. We say that a A-submodule $\mathfrak{a} \subseteq K$ is **fractional ideal** if there exists and $x \in A \setminus \{0\}$ such that $x \cdot \mathfrak{a} \subseteq A$. In this context, we call the ideals of A the **integral ideals**

Proposition 19.2. *Let A be a domain with $\mathfrak{a} \subseteq K$ a A-submodule. Then*

(1) If $\mathfrak{a}$ is finitely generated then it is a fractional ideal.

(2) If A is Noetherian and $\mathfrak{a}$ is a fractional ideal, then $\mathfrak{a}$ is finitely generated.

Proof. (1) Just multiply all the denominators of the generators of $\mathfrak{a}$.

(2) Because $x\mathfrak{a} \subseteq A$ is an ideal of A and so is finitely generated, $\mathfrak{a}$ is also finitely generated. □

For $S \subseteq K$ finite, we denote $(S) = \langle S \rangle_{A\text{-Mod}}$.

Definition 19.3. Let A be an integral domain and let $\mathfrak{a} \subseteq K$ an A-module. We say that $\mathfrak{a}$ is invertible if there exists a A-module $\mathfrak{b} \subseteq K$ such that $\mathfrak{ab} = A = (1)$.

Proposition 19.4. *Let $\mathfrak{a} \subseteq K$ be an invertible ideal. Then there exists a unique $\mathfrak{b} \subseteq K$ such that $\mathfrak{a} \cdot \mathfrak{b} = A$, and if fact, $\mathfrak{b} = (A : \mathfrak{a})$. Furthermore, $\mathfrak{a}$ is finitely generated.*

Proof. Let $\mathfrak{b} \subseteq K$ be a sub A-module with $\mathfrak{a} \cdot \mathfrak{b} = A$. Then

$$\mathfrak{b} \subseteq (A : \mathfrak{a}) = (A : \mathfrak{a}) \cdot A == (A : \mathfrak{a}) \cdot \mathfrak{a} \cdot \mathfrak{b} \subseteq A \cdot \mathfrak{b} = \mathfrak{b}.$$

Now, since $\mathfrak{a} \cdot \mathfrak{b} = (1)$, we get $1 = \sum_{j=1}^{n} \alpha_j \beta_j$. Then for each $x \in \mathfrak{a}$, we have

$$x = \sum_{j=1}^{n} (x\beta_j)\alpha_j = \sum_{j=1} c_j \alpha_j$$

for $c_j = x\beta_j \in A$. This shows that $\mathfrak{a}$ is generated by $\alpha_1, \ldots, \alpha_n$. □

Invertible ideals of A form an abelian group with identity element $A = (1)$. This is a general fact for an integral domain A.

Proposition 19.5. *Let A be an integral domain and $\mathfrak{a} \subseteq K$ be a fractional ideal. The following are equivalent:*

(i) $\mathfrak{a}$ *is invertible.*

(ii) $\mathfrak{a}$ *is finitely generated and $\mathfrak{a}_p$ is ($A_\mathfrak{p}$-)invertible for every $\mathfrak{p}$ prime.*

(iii) $\mathfrak{a}$ *is finitely generated and $\mathfrak{a}_\mathfrak{m}$ is ($A_\mathfrak{m}$-)invertible for every $\mathfrak{m}$ maximal.*

Proof. Exercise. □

Proposition 19.6. *Let $(A, \mathfrak{m})$ be a local integral domain. Then A is a DVR if and only if every nonzero fractional ideal is invertible.*

The global version of this proposition is that A is a Dedekind domain if and only if every nonzero fractional ideals are invertible.

20 October 19, 2016

20.1 Dedekind domains and fractional ideals

Proposition 20.1. *Let $(A, \mathfrak{m})$ be a local integral domain. Then A is a DVR if and only if every nonzero fractional ideals are invertible.*

Proof. For the forward direction, let $\mathfrak{m} = (x)$. Let $\mathfrak{a} \subseteq K = \operatorname{Quot}(A)$ be a non-zero fractional ideal. Then there exists $y \in A$ such that $y \cdot \mathfrak{a} \subseteq A$. This means that $y \cdot \mathfrak{a} = (x^r)$ for some r. Then $\mathfrak{a} = (x^r/y)$ and $\mathfrak{a}^{-1} = (y/x^r)$.

Now let us prove the converse. First A is Noetherian because every nonzero invertible integral ideal $\mathfrak{a} \subseteq A$ is finitely generated. We now show that every $(0) \neq \mathfrak{a} \subsetneq A$ is a power of $\mathfrak{m}$. Assume this fails, and let $\mathfrak{a}$ be a maximal counterexample, by the Noetherian hypothesis. Note that $\mathfrak{a} \subseteq \mathfrak{m}$. Also $\mathfrak{m}^{-1} = \mathfrak{m}^{-1} \cdot A \supseteq \mathfrak{m}^{-1} \cdot \mathfrak{m} = A$. Then $\mathfrak{m}^{-1}\mathfrak{a} \supseteq \mathfrak{a}$ and $\mathfrak{m}^{-1}\mathfrak{a} \subseteq \mathfrak{m}^{-1}\mathfrak{m} = A$.

If $\mathfrak{m}^{-1}\mathfrak{a} \supsetneq \mathfrak{a}$, then it is an integral ideal that is not a power of $\mathfrak{m}$. This contradicts the maximality of $\mathfrak{a}$. If $\mathfrak{m}^{-1}\mathfrak{a} = \mathfrak{a}$, then $\mathfrak{a} = \mathfrak{m}\mathfrak{a}$ so by Nakayama, $\mathfrak{a} = (0)$. This shows that every $(0) \neq \mathfrak{a} \subseteq A$ is a power of $\mathfrak{m}$, and this further implies $\dim A = 1$. □

Theorem 20.2. *Let A be an integral domain. Then A is Dedekind if and only if every nonzero fractional ideal is invertible.*

Proof. Just use Proposition 20.1 and localization techniques. □

Corollary 20.3. *In a Dedekind domain, nonzero fractional ideals form a group with respect to multiplication. This group is free abelian generated by prime ideals.*

Let A be a Dedekind domain. We write

$$\begin{aligned} \operatorname{Div}(A) &= \text{group of fractional ideals}, \\ \operatorname{PDiv}(A) &= \text{group of principal fractional ideals} = \{(x) : x \in K^\times\}, \\ \operatorname{Cl}(A) &= \operatorname{Div}(A)/\operatorname{PDiv}(A). \end{aligned}$$

The group $\operatorname{Cl}(A)$ is called the **class group**. This measures the "failure" of unique factorization of A.

Proposition 20.4. *If A is a Dedekind domain, the following are equivalent:*

(1) $\operatorname{Cl}(A) = (1)$.

(2) A is a UFD.

(3) A is a PID.

Proof. Clearly (3) implies (2) because you can go to ideals and factor and go back to elements. To show (2) $\Rightarrow$ (3), it is enough to show that primes are principal. Let $(0) \neq \mathfrak{p} \subseteq A$ be prime. Take any $0 \neq x \in \mathfrak{p}$. Then x factors into irreducibles $x = y_1 \cdots y_n$, with $n \geq 1$ because $x \notin A^\times$. Then there exists a j such that $y_j \in \mathfrak{p}$. Then $0 \neq (y_j) \subseteq \mathfrak{p}$. Because $\dim A = 1$, $(y_j) = \mathfrak{p}$. Finally (1) $\Leftrightarrow$ (3) is easy. □

Suppose you have a Dedekind domain $A \subseteq K$. Consider L a finite extension of K. Then we can look at the integral closure $\tilde{A}^L \subseteq L$.

$$\begin{array}{ccc} \tilde{A}^L & \hookrightarrow & L \\ \uparrow & & | \\ A & \hookrightarrow & K \end{array}$$

Then $\tilde{A}^L$ has dimension 1, and it is integrally closed in L. But we can't conclude that $\tilde{A}^L$ is Dedekind because don't know whether $\tilde{A}^L$ is Noetherian. This is true, but is not obvious. In a future assignment, you will prove that this is true if L/K is separable.

Theorem 20.5. *Let K be a number field (i.e., a finite extension of $\mathbb{Q}$). Let $\mathcal{O}_K$ be its ring of integers (= $\tilde{Z}^K$). We have:*

(1) $\mathcal{O}_K$ is a Dedekind domain.

(2) $\mathcal{O}_K^\times$ is a finitely generated abelian group.

(3) $\mathrm{Cl}(\mathcal{O}_K)$ is finite.

Proof. (1) See [AM] Proposition 9.5.

(2) This is not so bad: just use basic properties of heights of algebraic numbers.

(3) This is more delicate: it uses Minkowski's geometry of numbers. □

21 October 21, 2016

Today we are going to sketch the theory of modules of finite length. There are two key notions of "basic" modules.

- M is **simple** if the only submodules of M are 0 and M.
- M is **indecomposable** if $M = P \oplus Q$ implies $P = (0)$ or $Q = (0)$.

For example, $\mathbb{Z}/4$ as a $\mathbb{Z}$-module is indecomposable but not simple.

21.1 Length of a module

We are back to the general commutative algebra setting, where A is just a commutative ring. For M an A-module, a **chain** in M is a sequence $(M_0, \dots, M_r)$ of submodules such that

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_r = (0).$$

The **length** of this chain is r. A **decomposition series** for M is a maximal chain. This is equivalent to each M_i/M_{i+1} being simple. There is no reason for a decomposition to exist.

Proposition 21.1. *If M has a composition series of length n, then* every *composition series of M has length n. Moreover, every chain in M can be extended to a composition series.*

Proof. Define $l(M)$ as the least length of a composition series in M.

We first claim that $N \lneq M$ implies $l(N) < l(M)$. Given a minimal composition series $(M_0, \dots, M_r)$ in M, consider $N_j = N \cap M_j$. Then at least

$$N_0 = N \supseteq N_1 \supseteq \cdots \supseteq N_r = (0). \tag{$*$}$$

We also have

$$\frac{N_j}{N_{j+1}} = \frac{N \cap M_j}{N \cap M_{j+1}} \hookrightarrow \frac{M_j}{M_{j+1}}.$$

So N_j/N_{j+1} are either simple or (0). Deleting all the redundant chains, $(*)$ can be reduced to a composition series for N. But the embeddings are not all isomorphisms because $N \neq M$.

We now claim that all chains in M has length at most $l(M)$. Take any chain

$$M_0 \supsetneq M_1' \supsetneq \cdots \supsetneq M_{r-1}' \supsetneq M_r = (0).$$

By the first claim, this implies

$$l(M_0) > l(M_1') > \cdots > l(M_{r-1}') > 0.$$

Therefore $l(M) = l(M_0) \geq r$. This shows that every composition series of M has length $l(M)$.

Note also that if a chain has length $l(M)$ then it is a composition series, because if not, new terms can be inserted. This shows that each chain can be extend to a composition series, which has length $l(M)$. □

Definition 21.2. The maximal length $l(M)$ of a module M is called the **length** of M.

If $l(M) < \infty$, then it is the same as in the previous proof.

Proposition 21.3. *If $l(M) < \infty$, then M is Noetherian and Artinian.*

Proposition 21.4 (Jordan-Hölder theorem)**.** *Let M be a finite A-module of finite length, and let $(M_0, M_1, \ldots, M_r)$ and $(N_0, N_1, \ldots, N_k)$ be decomposition series for M. Then $r = k$ and the quotients M_j/M_{j+1} and M_i/M_{i+1} are isomorphic up to order.*

Proof. Induct on length. (We already know that $r = k$.) I'm not doing because it is too long. □

Proposition 21.5. *If $l(M) < \infty$ then M is a direct sum of indecomposable submodules.*

Proof. Induct on length. □

Lemma 21.6 (Splitting lemma)**.** *Let M, N be indecomposable, and let $\alpha : M \to N$ and $\beta : N \to M$. Let $\gamma = \alpha\beta \in \mathrm{End}_A(N)$. If γ is an isomorphism, then α and β are both isomorphisms.*

22 October 24, 2016

22.1 Field extensions

A **field extension** is an inclusion of fields $k \subseteq L$. It is called **finite** if L is a finite dimensional k-vector space. We denote this degree by $[L : k]$. Finite field extensions are algebraic.

Proposition 22.1. *If M/L is a finite extension and L/k is a finite extension, then M/k is finite and $[M : k] = [M : L][L : k]$.*

Given any $x_1, \dots, x_l \in L$, we will write $k[x_1, \dots, x_l]$ the sub k-algebra of L generated by $x_1, \dots, x_l$ and write $k(x_1, \dots, x_l)$ the subfield of L generated by $x_1, \dots, x_l$ and k.

Lemma 22.2. *Let L/k be a field extension. For any $x \in L$, we have an evaluation map $\mathrm{ev}_x : k[t] \to L$ given by $f(t) \mapsto f(x)$. This is a ring homomorphism and if x is transcendental over k then this gives an isomorphism $k[t] \cong k[x]$. If x is algebraic, then $\ker \mathrm{ev}_x = (h_x)$ for a unique monic irreducible $h_x \in k[x]$. This h_x is calledthe **minimal polynomial** of x over k and $k(x) = k[x] \cong k[t]/(\ker \mathrm{ev}_x)$. The degree of h_x is $\deg h_x = [k(x) : k]$.*

If $L = k(x)$ then we say that x is a **primitive element** for L/k. If such an x exists, L/k is called **primitive**.

Lemma 22.3 (Lifting lemma)**.** *Let $k(x)/k$ be a finite primitive extension, and let h_x be the minimal polynomial of x. Let $\sigma : k \to L$ be an isomorphism, with M/L a field extension. Note that σ extension to an isomorphism $\sigma' : k[x] \cong L[t]$. Then the set of roots of $\sigma'(h_x)$ in M is in bijection with the lifts $\tilde{\sigma} : k(x) \to M$ extending $\sigma : k \to L$.*

Proof. Without loss of generality, we may assume that $L = k$ and $\sigma = \mathrm{id}_k$. Then $k(x) \cong k[x]/(h_x)$ and so we have a bijection

$$\mathrm{Mor}_k(k(x), M) \longleftrightarrow \mathrm{Mor}_k(k[x]/(h_x), M) \longleftrightarrow \text{zeros of } h_x \text{ in } M. \qquad \square$$

22.2 Splitting fields

Let k be a field, and $f \in k[t]$.

Definition 22.4. Say that L/k is a **splitting field** for f

- if $f \in L[t]$ splits into linear factors, and
- L is minimal with respect to the above properties. (L is generated by the roots of f in L.)

Theorem 22.5. *Let $f \in k[t]$. Then there exists a splitting field L_f/k for f, and it is unique up to k-isomorphism. Moreover, $[L_f : k] \leq (\deg f)!$.*

Proof. Start by picking a irreducible factor g of f in $k[t]$. Then $k[s]/(g(s))$ is a field. Call this $k_1 = k(\overline{s})$. In this field, we have $f = (t - \overline{s})f_1(t)$. Now repeat this construction for f_1, and this gives a field k_2/k_1. Repeating this $\deg f$ times, we get $k_n = L_f$. In k_n, the polynomial f splits into linear factors, and L is generated by the roots of f.

We know show uniqueness. Let L/k be any splitting field for f. We construct an isomorphism $L_f \to L$ inductively. We have a map $k \to L$. We can extend it to $k_1 \to L$ by sending $\overline{s}$ to a root of g in L. In this way, we get a map $L_f \to L$. By construction, the image contains all roots of f, and this shows surjectivity.

The degree of L_f/k is

$$[L_f : k] = [k_n : k_{n-1}] \cdots [k_2 : k_1][k_1 : k] \leq 1 \cdot \cdots \cdot (\deg f) \leq (\deg f)!. \qquad \square$$

22.3 Normal field extensions

Definition 22.6. A field extension L/k is **normal** if it is algebraic and for every $x \in L$ the minimal polynomial $h_x \in k[t]$ factors into linear factors in $L[t]$.

Theorem 22.7. *If L/k is finite, then the following are equivalent:*

(1) L/k is normal.

(2) There exists an $f \in k[t]$ such that L/k is the splitting field of f.

(3) Every field extension M/L and k-map $\sigma : L \to M$ satisfies $\sigma(L) = L$.

23 October 26, 2016

Proposition 23.1. *Let L/k be a finite extension. Then the following are equivalent:*

(i) L/k is normal, i.e., for every $x \in L$, h_x splits into linear factors in $L[t]$.

(ii) L is the splitting field of some polynomial $f \in k[t]$.

(iii) For any M/L and k-algebra map $\sigma : L \to M$, the image is $\sigma(L) = L$.

(iv) For every $x_1, \dots, x_n \in L$, there exists an extension M/L such that h_{x_i} all split in M and any k-algebra map $\sigma : L \to M$ has $\sigma(L) = L$.

Proof. For (i) $\Rightarrow$ (ii), take generators $x_1, \dots, x_n$ for L as a k-algebra. Let $f = h_{x_1}, \dots, h_{x_n}$. Then this splits in $L[t]$, and the roots generate L.

For (ii) $\Rightarrow$ (iii), suppose L is a splitting field for f. Consider a map $\sigma : L \to M$. Then $\sigma(f(x)) = f(\sigma(x))$ because σ fixes K. Then σ sends roots of f to roots of f. Because L is generated by the roots of f, it follows that $\sigma(L)$ is also generated by roots of f. Also because $\sigma : L \to M$ is injective, $\sigma(L) = L$.

For (iii) $\Rightarrow$ (iv), let M be the splitting field of $h_{x_1} \cdots h_{x_n}$ over L. Then both conditions are obviously satisfied.

For (iv) $\Rightarrow$ (i), consider any $x \in L$. We extend this to a set of generators $x, x_2, \dots, x_n$ of L/k. Take M such that $h_x, h_{x_2}, \dots, h_{x_n}$ split in M and any $\sigma : L \to M$ has $\sigma(L) = L$. Let $y \in M$ be any root of h_x. Then there is a map $\sigma : k(x) \cong k(y)$ in M, and we can extend this to $\sigma' : k(x, x_2, \dots, x_n) \to M$. Then $\sigma'(L) = L$ and $y \in \sigma'(L)$, so $y \in L$. This shows that h_x splits in L. $\square$

Proposition 23.2. *Let L/k and M/L be field extensions. If M/k is normal, then M/L is normal (but L/k might not be normal).*

Even if L/k and M/L are both normal, M/k need not be normal.

23.1 Separable field extensions

This is a property that is satisfied by most of the field extensions we care about. Let $f \in k[t]$ be a polynomial.

Definition 23.3. f is **separable** if f has exactly $\deg f$ distinct roots in the splitting field L_f for f/k.

f is separable if and only if $\gcd(f, f') = 1$, where f' is the formal derivative. If f is irreducible, then f is separable if and only if $f' \neq 0 \in k[t]$. This is mostly true, but for instance, $t^p - x \in k[t]$ has zero derivative if t has characteristic p.

Definition 23.4. An algebraic extension L/k, say that L/k is **separable** if for all $x \in L$, the minimal polynomial h_x is separable.

Theorem 23.5 (Primitive element theorem)**.** *If L/k is finite and separable, then there exists an $x \in L$ such that $L = k(x)$.*

Proof. If k is a finite field, then $L^\times$ is a cyclic group, and so we can take x to be the generator.

Now we assume that k is infinite. It is enough to show when $L = k(y, z)$, because we can induct on the number of generators. Take $x = y - \lambda z$ where $y - y' \neq \lambda(z - z')$ for every $h_y(y') = h_z(z') = 0$ with $y' \neq y$ and $z' \neq z$ (in the splitting field of $h_y h_z$).

The polynomials $h_z \in k[t] \subseteq k(x)[t]$ has z as a root, and $H(t) = h_y(x + \lambda t) \in k(x)[t]$ also has z as a root. Then $\gcd(H, h_z) \in k(x)[t]$ also has z as a root. But by the genericity condition, it they have no other common roots. This hsows that $\gcd(H, h_z)$ has degree 1, and thus $z \in k(x)$. Then $y \in k(x)$. □

Proposition 23.6. *For field extensions, L/k and M/L are both separable if and only if M/k are separable.*

Example 23.7. Let $k = \mathbb{F}_p$. Then $f(t) = t^{p^r} - t$ has derivative -1 so it is separable. Consider the splitting field L_f, which is the finite extension of $\mathbb{F}_p$. Then $|L_f| = p^n$ for some n. Consider the map $\sigma : x \mapsto x^p$ that is an automorphisms of L_f. Notice that $\sigma^r(x) = x$ for any root x of f, and so the roots of f form a field. This has to be L_f, and thus $|L_f| = p^r$. We call this **finite field** $L_f = \mathbb{F}_{p^r}$. If L is any other finite field with $|L| = p^r$, then $L^\times$ is a finite cyclic group of order $p^r - 1$. Then every $x \in L$ satisfies $x^{p^r} - x$ and so $L \cong \mathbb{F}_{p^r}$. That is, the field with p^r elements is unique up to isomorphism.

24 October 28, 2016

24.1 Galois extensions

Definition 24.1. If L/k is normal and separable, then we say that L/k is **Galois**.

Lemma 24.2. *If L/M and M/k are finite extensions and L/k is Galois, then L/M is Galois. (M/k is not necessarily Galois.)*

Lemma 24.3. *If L/k is finite and Galois, then we can write $L = k(x)$ where the minimal polynomial h_x of x splits into distinct linear factors in $L[t]$.*

Proof. By the primitive element theorem, we can write $L = k(x)$ for some x. Then h_x splits because L/k is normal, and there are no repeated factors because L/k is separable. □

Definition 24.4. If L/k is a field extension, then we denote

$$\mathrm{Gal}(L/k) = \{k\text{-automorphisms of } L\} = \{\text{field automorphism of } L \text{ that fix } k\}.$$

This naturally forms an group.[1]

Lemma 24.5 (Counting automorphisms)**.** *If L/k is finite and $[L : k] = n$, then $|\mathrm{Gal}(L/k)| \le n$. Moreover, we have equality if L/k is Galois.*

Proof. We use the lifting lemma. Let $L = k(x_1, \dots, x_r)$. Let $k_j = k(x_1, \dots, x_j)$. Then we have a tower

$$k_0 \subseteq k_1 \subseteq k_2 \subseteq \cdots \subseteq k_r = L$$

with each step being a extension generated by a single element. By inductive application of the lifting lemma, the number of k-maps $L \to L$ is at most

$$[k_1 : k][k_2 : k_1] \cdots [k_r : k_{r-1}] = [k_r : k] = n.$$

If L/k is Galois, then $L = k(x)$ for x in the previous lemma. Then the lifting lemma says that

$$\#\{k\text{-maps } k(x) \hookrightarrow L\} = \#\{\#\text{ of roots of } h_x \text{ in } L\} = \deg h_x = n. \qquad \square$$

Our goals are:

- showing that $\#\,\mathrm{Gal}(L/k) = [L : k]$ if and only if L/k is Galois.
- for a finite Galois extension L/k, showing that there is a one-to-one correspondence

$$\begin{pmatrix}\text{intermediate fields}\\ k \subseteq M \subseteq L\end{pmatrix} \iff \begin{pmatrix}\text{subgroups } H\\ \text{of } \mathrm{Gal}(L/k)\end{pmatrix}$$

$$M \longmapsto \mathrm{Gal}(L/M)$$

$$L^H \longmapsfrom H$$

[1] Some people define this only when L/k is Galois.

Definition 24.6. If $H \subseteq \mathrm{Gal}(L/k)$ then define the fixed field $L^H = \{x \in L : \sigma(x) = x \text{ for every } \sigma \in H\}$.

It is clear that $H \leq \mathrm{Gal}(L/L^H)$ and $L^{\mathrm{Gal}(L/M)} \supseteq M$.

Lemma 24.7 (Artin)**.** *Let M be a field, and H be a finite group of field automorphisms of M. Then M/M^H is finite Galois of degree $\#H$ and $\mathrm{Gal}(M/M^H) = H$.*

Proof. Let $k = M^H$. We first prove that M/M^H is Galois. Pick a $x \in M$, and we want to show that h_x splits into distinct factors in $M[t]$. Let H_x be the stabilizer of x in H. Then

$$\prod_{[\sigma] \in H/H_x} (t - \sigma(x)) \in M^H[t]$$

splits into distinct linear factors. This shows that M/M^H is Galois, and also shows that for any $x \in M$, $k(x)/k$ has degree at most $\#H = n$. But we can't pick a primitive element yet because we don't know that M/M^H is finite.

Choose $x \in M$ with $[k(x) : k]$ maximal. This is possible because $[k(x) : k] \leq n$ always. We claim that $M = k(x)$. If $y \in M \setminus k(x)$ then $k(x, y) \supsetneq k(x)$ and $k(x, y) = k(z)$ for some $z \in M$ by the primitive element theorem. Then $k(z) \supsetneq k(x)$ contradicts the maximality of x. This shows that $M = k(x)$, and so $[M : k] \leq n$.

Now we have

$$[M : M^H] \leq n = \#H \leq \#\,\mathrm{Gal}(M/M^H) \leq [M : M^H].$$

Therefore everything must be equalities, and in particular, $[M : M^H] = n$ and $\mathrm{Gal}(M/M^H) = H$. □

Corollary 24.8. *Let L/k be a finite Galois extension and let $H = \mathrm{Gal}(L/k)$. Then $L^H = k$.*

Proof. We have $L^H \supseteq k$. By the previous theorem, we have

$$[L : L^H] = \#H = \#\,\mathrm{Gal}(L/k) = [L : k].$$

So $[L^H : k] = 1$, i.e., $L^H = k$. □

Corollary 24.9. *Let L/k be finite with $[L : k] = \#\,\mathrm{Gal}(L/k)$. Then L/k is Galois.*

Proof. $H = \mathrm{Gal}(L/k)$. Then we have $[L : L^H] = \#H = [L : k]$ by Artin's lemma. So $L^H = k$, and Artin's lemma implies that $L/L^H = L/k$ is Galois. □

I am now going to try and state the fundamental theorem of Galois theory.

Theorem 24.10 (Fundamental theorem of Galois theory)**.** *Let L/k be a finite Galois extension. We have a correspondence between an intermediate field M and a subgroup H of $\mathrm{Gal}(L/k)$, with the following properties:*

(i) *It is order-reversing, i.e.,* $M \subseteq M'$ *if and only if* $H \supseteq H'$.

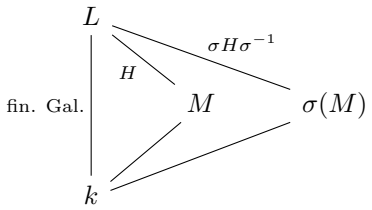
(ii) $[L : M] = \#\operatorname{Gal}(L/M)$ *for each* M.

(iii) $[L^H : k] = [\operatorname{Gal}(L/k) : H]$ *for each* H.

Why do we have a bijection? We only need to show that $L^{\operatorname{Gal}(L/M)} = M$. By Corollary 24.8, L/M is Galois. Then by Artin's lemma, $\operatorname{Gal}(L/L^{\operatorname{Gal}(L/M)}) = \operatorname{Gal}(L/M)$.

25 October 31, 2016

If you have a finite Galois extension L/k and an intermediate field extension M, then M/k need not be normal. So an automorphism $\sigma \in \operatorname{Gal}/k$ might move M around.



Then the Galois group $\operatorname{Gal}(L/\sigma(M))$ is given by the conjugation of $\operatorname{Gal}(L/M)$. So M/k is Galois if and only if $H = \operatorname{Gal}(L/M)$ is normal in $G = \operatorname{Gal}(L/k)$. In this case, we have an isomorphism

$$\operatorname{Gal}(L/k)/\operatorname{Gal}(L/M) \to \operatorname{Gal}(M/k)$$

that is given by restriction.

25.1 Examples of field extensions

Lemma 25.1. *Let $f \in K[t]$ be irreducible and separable. Then $G_{f/K} = \operatorname{Gal}(K_f/K)$ acts transitively on the roots of f in K_f.*

Proof. It follows from the lifting lemma. □

Lemma 25.2. *For $f \in K[t]$ irreducible and separable, by action on the roots of f, we can see $G_{f/K}$ as a transitive subgroup of S_d for $d = \deg f$.*

Example 25.3. Let $\operatorname{char} K \neq 2$ and $d = 3$. Let $f \in K[t]$ be irreducible and separable. Then $G_{f/K}$ is a transitive subgroup of S_3. The subgroups of S_3 up to conjugation are:

Order	1	2	3	6
Example	$\{e\}$	$\langle(12)\rangle$	$\langle(123)\rangle$	S_3
# of conjugations	1	3	1	1
Transitive?	No	No	Yes	Yes

Table 1: Subgroups of S_3 up to conjugation

But in practice, how do you know which one it is? Consider the discriminant, which is defined as

$$\Delta_f = \{(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)\}^2 = (-1)^{d(d-1)/2} \operatorname{Res}(f, f'),$$

where $\alpha_1, \alpha_2, \alpha_3$ are the roots of f. Let

$$\delta_f = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3),$$

for this arbitrary ordering. If $\sigma \in G_{f/K}$ is a 3-cycle, then $\sigma(\delta_f) = \delta_f$. So in the case that $G_{f/K} = \langle (123) \rangle$, the Galois group fixes δ_f, and this means that $\delta_f \in K$. On the other hand, if $G_{f/K} = S_3$ then $\tau = (12)$ acts on δ_f as $\tau(\delta_f) = -\delta_f$. Then $\delta_f \notin K$. Therefore

$$G_{f/K} \cong \begin{cases} S_3 & \text{if } \Delta_f \text{ is not a square in } K \\ A_3 & \text{if } \Delta_f \text{ is a square in } K. \end{cases}$$

For instance, if $K = \mathbb{Q}$ then $f = t^3 + t^2 - 3$, which is irreducible by rational root test, has discriminant $\Delta_f = -231 = -3 \cdot 7 \cdot 11$. So $\mathrm{Gal}(f/\mathbb{Q}) \cong S_3$.

Lemma 25.4. *S_n is generated by any of the following:*

(i) transpositions.

(ii) transpositions of the form $(1r)$ for $2 \le r \le n$.

(iii) transpositions of the form $(r(r+1))$ for $1 \le r \le n-1$.

(iv) (12) and $(123 \cdots n)$.

Lemma 25.5. *Let $f \in K[t]$ be irreducible and separable. Suppose $p = \deg f$ is prime. Then $G_{f/K}$ contains a p-cycle of S_p.*

Proof. $\deg f = p$ implies that $p \mid [K_f : K] = \#G_{f/K}$. Then by Cauchy, there exists a $\sigma \in G_{f/K}$ of order p. Since p is prime, then σ is a p-cycle. □

Lemma 25.6. *Let $f \in \mathbb{Q}[t]$ be irreducible (hence separable). Suppose $\deg f = p$ is prime and f has exactly 2 non-real roots. Then $G_{f/\mathbb{Q}} \cong S_p$.*

Proof. Complex conjugation gives a transposition and there is a p-cycle. These generate the whole S_p. □

Example 25.7. Let $K = \mathbb{Q}$ and $f = t^5 - 6t + 3$. By Eisenstein at 3, this polynomial is irreducible. Also f has three real roots exactly after doing calculus. Therefore $\mathrm{Gal}_{f/\mathbb{Q}} \cong S_5$.

26 November 2, 2016

Definition 26.1. A field K is **perfect** if every irreducible $f \in K[t]$ is separable.

For example, $K = \mathbb{F}_p(s)$ is not perfect because $f(t) = t^p - s$ is irreducible but it factors as $(t - \sqrt[p]{s})^p$ in K_f. Fields of characteristic zero are perfect, and finite fields are perfect. Also algebraically closed fields are clearly separable.

26.1 Solvability by radicals

All fields in this section has characteristic zero.

Definition 26.2. A field extension L/K is **pure radical** of exponent n if there exists $\gamma_1, \dots, \gamma_r \in L$ such that for each i, $\gamma_i^n \in K$ and $L = K(\gamma_1, \dots, \gamma_r)$. L/K is **radical** if there exists a tower

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m = L$$

such that K_i/K_{i-1} is pure radical for each i.

Definition 26.3. We say that $f \in K[t]$ is **solvable by radicals** if there exists a radical extension L/K such that $K_f \subseteq L$.

For example, consider the case $K = \mathbb{Q}$, $d = \deg f$ with f irreducible. If $d = 1$ then it is always solvable. If $d = 2$, then the roots are $(-b \pm \sqrt{b^2 - 4ac})/2a$ and so f is always solvable. If $d = 3$ then it is also always solvable, and it was found by Ferro and first published by Cardano. The case $d = 4$ was solved by Ferrari, and for $d = 5$ it was fist proved that there are non-solvable polynomials by Abel.

Let us write

$$\mu_n = \{\epsilon \in K_{t^n - 1} : \varepsilon^n = 1\},$$

and this under $\times$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z}, +)$.

Lemma 26.4. *The extension $K(\mu_n)/K$ is Galois and $\mathrm{Gal}(K(\mu_n)/K)$ is a subgroup of $\mathrm{Aut}(\mu_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.*

Proof. It is Galois because $K(\mu_n) = K_{t^n-1}$ and $\operatorname{char} K = 0$. Let $\sigma \in G = \mathrm{Gal}(K(\mu_n)/K)$. Then σ acts on μ_n and $\sigma(\epsilon \cdot \epsilon') = \sigma(\epsilon)\sigma(\epsilon')$. So we get a map

$$G \to \mathrm{Aut}(\mu_n); \quad \sigma \mapsto \sigma|_{\mu_n}.$$

This is injective because μ_n generates the extension. □

Definition 26.5. A pure radical extension L/K of exponent n is **Kummer** if $\mu_n \subseteq K$. (This is for some admissible n.)

Lemma 26.6. *If L/K is Kummer of exponent n, then it is Galois, abelian, and $\mathrm{Gal}(L/K)$ has exponent dividing n.*

Proof. Write $L = K(\gamma_1, \ldots, \gamma_r)$ with $\alpha_i = \gamma_i^n \in K$. (Assume without loss of generality that $\gamma_i \neq 0$.) Conjugates of γ_i are among $\gamma_i \mu_n$, which is the roots of $t^n - \alpha_i$. So L/K is Galois.

Let $G = \mathrm{Gal}(L/K)$. Define

$$\delta : G \to \mu_n \times \cdots \times \mu_n = (\mu_n)^r; \quad \sigma \mapsto \Big(\frac{\sigma(\gamma_i)}{\gamma_i}\Big).$$

Note that δ is a group morphism, and it is injective. Therefore $\mathrm{Gal}(L/K)$ is abelian. □

Every time you have a Galois extension with abelian Galois group, it is actually Kummer. This is the whole point the Kummer theory, but we are not going to do this.

Definition 26.7. A radical extension L/K is **prepared** if it has a tower

$$K \subseteq L_0 \subseteq \cdots \subseteq L_r = L$$

and an integer $n \geq 1$ satisfying

(1) L/K is normal (and hence, Galois),

(2) $L_0 = K(\mu_n)$,

(3) for each $1 \leq i \leq r$, the extension L_i/L_{i-1} is Kummer of exponent n.

Lemma 26.8. *Let L/K be radical. Then there is an extension L'/K prepared radical extension with $L' \supseteq L$.*

I will prove this next time.

Theorem 26.9. *Let K be of characteristic 0, and let $f \in K[t]$ be irreducible. Suppose that f is solvable by radicals. Then $G_{f/K}$ is a solvable group.*

Proof. Let $K_f \subseteq L$ with L/K radical. Lemma 26.8 tells us that we can assume L/K is prepared. Then Lemma 26.4 and Lemma 26.6 gives us a chain of subgroups

$$\{1\} \subseteq H_1 \subseteq H_2 \subseteq \cdots \subseteq H_r = \mathrm{Gal}(L/K)$$

with H_{i+1}/H_i abelian. Thus $\mathrm{Gal}(L/K)$ is solvable. Then $\mathrm{Gal}(K_f/K)$ is solvable because it is a quotient of $\mathrm{Gal}(L/K)$. □

Corollary 26.10. *The general quintic equation over $\mathbb{Q}$ is not solvable by radicals.*

27 November 4, 2016

27.1 Representations of finite groups

Let G be a finite group, and let k be a field, both fixed.

Definition 27.1. A (k-linear finite dimensional) **linear representation** of G is a pair (V, ρ) with V a finite dimensional k-vector space and $\rho : G \to \mathrm{GL}(V) = \mathrm{Aut}_k(V)$ a group morphism.

There are two different (equivalent) points of view:

(i) Linear action: V is a k-vector space and G acts on V in a k-linear way, i.e., $g \cdot (x + \lambda y) = g \cdot x + \lambda g \cdot y$.

(ii) Modules over group rings: If we define the group ring $R = k[G]$, then a representation of G is a k-vector space V with a compatible structure of a left R-module.

Clearly (k, ρ_{triv}) is a representation. If S is a finite G-set, then G has a natural representation (V_S, ρ_S) given by $e_g \cdot \epsilon_s = \epsilon_{g \cdot s}$.

Example 27.2. The vector space $V_{\text{reg}} = R$ is a left R-module and so this gives a representation. This is called the **regular representation**.

If V and V' are representations, then $\mathrm{Hom}_k(V, V')$ is a k-vector space with a G-action given by

$$\rho_H(g)(f) = \rho'(g) \circ f \circ \rho(g^{-1}).$$

If (V, ρ) is a representation and $W \subseteq V$ is a subspace such that W is ρ-stable, then $(W, \rho(\ )|_W)$ is a representation. Also, if V and V' are representations, then both $V \oplus V'$ and $V \otimes V'$ have natural G-action. If (V, ρ) is a representation, then $(V^\vee, \rho^\vee)$ defined as $\rho^\vee(g) = \rho(g^{-1})^t$ is a representation. Note that now we have duals, homs, and tensor product. It turns out that the induced representations on $\mathrm{Hom}_k(W, V)$ and $V \otimes W^\vee$ are compatible.

Definition 27.3. A representation $(V, \rho) \neq 0$ is called **simple** if its only subrepresentations are 0 and V. A representation $(V, \rho) \neq 0$ is called **irreducible** if it has no nontrivial direct sum decomposition.

Simple implies irreducible, but the converse is not true. For instance, let $G = \mathbb{Z}/p\mathbb{Z}$ and $k = \mathbb{F}_p$ with $V = k^2$. Then $\mathrm{GL}(V) = \mathrm{GL}_2(k)$ and let ρ be given by

$$\rho : G \to \mathrm{GL}(V); \quad \bar{n} \mapsto \begin{bmatrix} 1 & \bar{n} \\ 0 & 1 \end{bmatrix}.$$

The trivial representation ρ_{triv} is a subrepresentation because ρ stabilizes the x axis. But it is irreducible.

Definition 27.4. Let (V, ρ) and (V', ρ') be representations. A **morphism** is a k-linear map $f : V \to V'$ such that for all $g \in G$,

$$f \circ \rho(g) = \rho'(g) \circ f.$$

Equivalently, one can consider it as a morphism of left R-modules. We are going to denote this by $\mathrm{Hom}_G(V, V')$. This is naturally a subset of $\mathrm{Hom}_k(V, V')$, and using the G-action on $\mathrm{Hom}_k(V, V')$, we have $\mathrm{Hom}_G(V, V') = \mathrm{Hom}_k(V, V')^G$.

Lemma 27.5 (Schur's lemma)**.** *Assume k is algebraically closed, and let V, W be simple representations. Then*

$$\mathrm{Hom}_G(V, W) = \begin{cases} 0 & \text{if } V \ncong W \\ k & \text{if } V \cong W \end{cases}.$$

Proof. Note that for every $f \in \mathrm{Hom}_G(V, W)$, $\ker f = 0$ or V and $\operatorname{im} f = 0$ or W because V and W are simple. Now if $V \ncong W$, then it is automatic that $\ker f \neq V$ and $\operatorname{im} f \neq 0$. Then $\ker f = 0$ and $\operatorname{im} f \neq W$. So $V \cong W$. Suppose that $V = W$, and let $f \in \mathrm{Hom}_G(V, V)$. Because k is algebraically closed, there exists a $\lambda \in k$ that is an eigenvalue for f. Then $\ker(f - \lambda I) \neq 0$. Observe that $\lambda I \in \mathrm{Hom}_G(V, V)$ and so $\ker(f - \lambda I) = V$. So $f = \lambda I$. □

Suppose $\mathrm{char} \nmid n = \#G$. For an irreducible representation (V, ρ), define $\mathrm{Avg}_v \in \mathrm{Hom}(V, V^G)$ as

$$\mathrm{Avg}_v(x) = \frac{1}{n} \sum_{g \in G} \rho(g)(x).$$

Note that $\mathrm{Aug}_v(x) \in V^G$ and $\mathrm{Avg}_v|_{V^G} = I_{V^G}$. Also it is a projection, i.e., idempotent.

28 November 7, 2016

Last time we discussed representations and this averaging operator. Assuming that $\operatorname{char}(k) \nmid n = \#G$, from a representation (V, ρ) we define the k-linear map

$$\operatorname{Avg}_V : V \to V^G \subseteq V; \quad x \mapsto \frac{1}{n} \sum_{g \in G} \rho(g)(x).$$

Then $\operatorname{Avg}_V |_{V^G} = \operatorname{Id}_{V^G}$. Also $(\operatorname{Avg}_V)^2 = \operatorname{Avg}_V$. So Avg is a projection onto V^G. In the case $H = \operatorname{Hom}_k(W, V)$, the fixed space is $H^G = \operatorname{Hom}_G(W, V)$. Then

$$\operatorname{Avg}_H : \operatorname{Hom}_k(W, V) \to \operatorname{Hom}_G(W, V).$$

Theorem 28.1 (Maschke)**.** *Suppose* $\operatorname{char}(k) \nmid n$*. Then every finite dimensional* k*-linear representation of* G *can be decomposed as a direct sum of simple representations (i.e., "irreducible = simple").*

Proof. Let (V, ρ) be a representation, and let $W \subseteq V$ be a subrepresentation. The goal is to find a subrepresentation $U \subseteq V$ such that $V = W \oplus U$. Note that if you have an idempotent operator, then there is a direct decomposition into its image and kernel.

Let $f : V \to W \subseteq V$ be any k-linear projection, i.e., $f|_W = \operatorname{id}_W$. Let $\pi = \operatorname{Avg}_H(f)$ where $H = \operatorname{Hom}_k(V, W)$. Then $\pi \in \operatorname{Hom}_G(V, W)$ and $\pi : V \to W \subseteq V$. We claim that $\pi|_W = \operatorname{Id}_W$. For $x \in W$,

$$\begin{aligned}\pi(x) &= \frac{1}{n} \sum_g (\rho_H(g)(f))(x) = \frac{1}{n} \sum_g (\rho(g) \circ f \circ \rho(g^{-1}))(x) \\ &= \frac{1}{n} \sum_g \rho(g) \circ f(\rho(g^{-1})(x)) = \frac{1}{n} \sum_g \rho(g)(\rho(g^{-1})(x)) = \frac{1}{n} \sum_g x = x.\end{aligned}$$

So take $U = \ker(\pi)$. This works. □

28.1 Structure of finite representations

Now let's assume:

- k is algebraically closed (for Schur's lemma),
- $\operatorname{char}(k) \nmid n$ (for Maschke's theorem).

Corollary 28.2. *Let* V *be a representation, and* W *be an irreducible representation. Then* $\dim_k \operatorname{Hom}_G(V, W)$ *is equal to the number of copies of* W *in the direct sum decomposition of* V*. In particular, this number is independent of the choice of a direct sum decomposition.*

Proof. Write $V = W_0^{a_0} \oplus W_1^{a_1} \oplus \cdots \oplus W_r^{a_r}$ with $W = W_0, W_i$ non-isomorphic irreducible. Then

$$\begin{aligned}\operatorname{Hom}_G(V, W) &= \operatorname{Hom}_G(W_0^{a_0} \oplus \cdots \oplus W_r^{a_r}, W_0) = \bigoplus_{i=0}^{r} \operatorname{Hom}_G(W_i, W_0)^{a_i} \\ &= \operatorname{Hom}_G(W_0, W_0)^{a_0} \cong k^{a_0}\end{aligned}$$

by Schur. □

Corollary 28.3. *The direct sum decomposition into irreducibles is unique up to isomorphism.*

Corollary 28.4. *Up to isomorphism, there are only finitely many irreducible representations of G over k. Furthermore, if W is irreducible then W appears $\dim_k W$ times in V_{reg}. In particular,*

$$n = \dim V_{\text{reg}} = \sum_{W \text{ irr.}} (\dim W)^2.$$

Proof. By definition,

$$\text{Hom}_G(V_{\text{reg}}, W) \cong \text{Hom}_{R\text{-mod}}(R, W) \cong W. \qquad \square$$

Example 28.5. Take $G = S_3$, and $\text{char}(k) \neq 2, 3$. Let's find representations.

- $V_{\text{triv}} = (k, \rho_{\text{triv}})$ with $\dim V_{\text{triv}} = 1$.
- $V_{\text{sgn}} = (k, \rho_{\text{sign}})$ with $\dim V_{\text{sign}} = 1$ given by $\rho_{\text{sign}}(\sigma)(x) = \text{sign}(\sigma) \cdot x$.

Now we are missing either four 1-dimensional representations or one 2-dimensional representation. We have the permutation on on $X = \{1, 2, 3\}$. This representation (V_X, ρ_X) has dimension 3. Consider the averaging operator $\text{Avg}_{V_X} : V_X \to V_X^G \subseteq V_X$. We have

$$V_X^G = \text{span}(\text{Avg}_{V_X}(e_i)) = \langle (1, 1, 1) \rangle.$$

Let $W = \ker(\text{Avg}_{V_x}) = \langle e_1 - e_2, e_1 - e_3 \rangle$. Is W irreducible? Using bases, it is possible to check that W does not split into two 1-dimensional representations. So we have all the irreducible representations, because $1^2 + 1^2 + 2^2 = 6$.

29 November 9, 2016

Today we continue with examples. Assume $k = \mathbb{C}$ for convenience. In general, for a (abelian) group, its **dual** is defined as

$$G^\vee = \mathrm{Mor}_{\mathrm{Grp}}(G, \mathbb{C}^\times) = \{\text{1-dimensional representations of } G\}.$$

Note that if $\rho_1 \neq \rho_2 \in G^\vee$ then $\rho_1 \ncong \rho_2$ because the eigenvalue of $\rho_i(1)$ is simply $\rho_i(1)$. Therefore we get an inclusion $G^\vee \hookrightarrow \{\text{irr. rep. of } G\}$.

Example 29.1. Consider $G = \mathbb{Z}/n\mathbb{Z}$. Here are some elements of $G^\vee$: Let $a \in \mathbb{Z}/n\mathbb{Z}$ and define $\psi_a : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^\times$ as map $r \mapsto e^{2\pi i r a/n}$. Thus we get an injection

$$\psi : \mathbb{Z}/n\mathbb{Z} = G \hookrightarrow G^\vee; \quad a \mapsto \psi_a.$$

So we get n 1-dimensional irreducible representations of $G = \mathbb{Z}/n\mathbb{Z}$. Because the square of the dimensions add up to n, this is all.

Example 29.2. Consider an arbitrary abelian group $G = \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_t\mathbb{Z}$. Let us look at $G^\vee$ again. It takes a minute to see $G^\vee \cong (\mathbb{Z}/n_1\mathbb{Z})^\vee \times \cdots \times (\mathbb{Z}/n_t\mathbb{Z})^\vee$. So $G^\vee$ gives $n = n_1 \cdots n_t$ representations, and there are no more.

Corollary 29.3. *For $k = \mathbb{C}$, if G is finite abelian, then all irreducible representations of G are 1-dimensional, and there are $n = \#G$ of them.*

29.1 Characters

Now we work in $\mathbb{C}$, because we want complex conjugation. Let G be a finite group and $n = \#G$.

Definition 29.4. A map $\xi : G \to \mathbb{C}$ is a **class function** if it is constant on conjugacy classes of G.

Let r be the number of conjugacy classes of G, and let $\Omega \cong \mathbb{C}^r$ be the space of class functions. We define a inner product on Ω as

$$(\psi, \xi) = \frac{1}{n} \sum_{g \in G} \psi(g)\overline{\xi(g)}.$$

For (V, ρ) a representation, define

$$\chi_V = \chi_\rho = \mathrm{tr}(\rho(-)) : G \to \mathbb{C}.$$

Because trace is invariant under conjugation, $\chi_V \in \Omega$. We call χ_V the **character** of the representation. Note that $V \cong W$ implies $\chi_V = \chi_W$. There are some basic properties:

- $\chi_{V \oplus W} = \chi_V + \chi_W$.

- $\chi_{V\otimes W} = \chi_V \cdot \chi_W$.
- $\chi_{V^\vee} = \overline{\chi_V}$.
- $\chi_V(e) = \dim V$.
- $\chi_{\text{triv}} = 1$.

Theorem 29.5. $(\chi_V, \chi_W) = \dim_{\mathbb{C}} \operatorname{Hom}_G(W, V)$.

Proof. Note that if U is a representation, then $\text{Avg}_U : U \to U^G \subseteq U$ is a projection onto U^G. So

$$\dim U^G = \operatorname{Tr}(\text{Avg}_U) = \operatorname{Tr}\left(\frac{1}{n}\sum_g \rho_U(g)\right) = \frac{1}{n}\sum_g \operatorname{Tr}(\rho_U(g)) = \frac{1}{n}\sum_g \chi_U(g).$$

Now take $U = V \otimes W^\vee = \operatorname{Hom}(W, V)$. Then

$$(\chi_V, \chi_W) = \frac{1}{n}\sum_g \chi_V(g)\cdot\overline{\chi_W(g)} = \dim \operatorname{Hom}(W,V)^G = \dim_{\mathbb{C}} \operatorname{Hom}_G(W,V). \square$$

This is incredibly useful because this Hom detects how many irreducible representations they have.

Corollary 29.6. *The set $\{\chi_V\}$ for V irreducible are orthonormal. In other words, $(\chi_V, \chi_W) = \delta_{V\cong W}$ for V and W irreducible.*

Proof. Schur. $\square$

Corollary 29.7. *If V and W are representations with $\chi_V = \chi_W$, then $V \cong W$ as representations.*

Lemma 29.8. *Let $\psi \in \Omega$ and (V, ρ) be a representation. Define*

$$f_{\psi,V} = \sum_g \psi(g)\rho(g) \in \operatorname{End}_{\mathbb{C}}(V).$$

Then $f_{\psi,V} \in \operatorname{End}_G(V)$.

Proof. Let $h \in G$. Then

$$\begin{aligned} f_{\psi,V}\circ\rho(h) &= \sum_g \psi(g)\rho(gh) = \sum_g \psi(hgh^{-1})\rho(hg) \\ &= \sum_g \psi(g)\rho(hg) = \rho(h)\circ f_{\psi,V}. \end{aligned}$$ $\square$

Theorem 29.9. *The set $\{\chi_V : V \text{ is irr.}\}$ is an orthonormal basis for Ω. In particular, the number of irreducible representations is r.*

Proof. Let $\psi \in \Omega$ and suppose $(\psi, \chi_V) = 0$ for every V representation. We need to show that $\psi = 0$. Take any irreducible V. The previous lemma and Schur implies that $f_{\psi,V} = \lambda_V \cdot \mathrm{Id}_V$. Then

$$\lambda_V \cdot \dim V = \mathrm{Tr}(f_{\psi,V}) = n \cdot (\psi, \chi_V) = 0$$

by the hypothesis. Thus if V is irreducible, then $\lambda_V = 0$ and so $f_{\psi,V} = 0$. By linearity, for every representation W, $f_{\psi,W} = 0$. Take $W = V_{\mathrm{reg}}$. Then we get the equation

$$\sum_g \psi(g) e_g = 0.$$

Therefore $\psi \equiv 0$. □

30 November 11, 2016

Recall that so far we know that $\{\chi_V : V \text{ irred.}\}$ is an orthonormal basis for Ω. Moreover, given any representation U and V irreducible, we have that (χ_U, χ_V) is the number of copies of V in U. This is called "orthogonality I".

Corollary 30.1. *If $(\chi_V, \chi_V) = 1$, then V is irreducible.*

Corollary 30.2. *Let G be a finite group. Then G is abelian if and only if all irreducible representations of G are 1-dimensional.*

Proof. We know that G is abelian if and only if $n = r$, where n is the order of G and r is the number of conjugacy. Now use the formula $n = \sum \dim^2$. □

Before, with some work, we proved the forward direction of this corollary.

Definition 30.3. Let $V_1, \dots, V_r$ be the irreducible representations of G. Let $g_1, \dots, g_r$ be representatives for the conjugacy classes in G. In particular, $G = \bigcup C_{g_i}$ where C_{g_i} denotes the conjugacy classes. We define the **character table** of G as the matrix

$$T = [\chi_{V_i}(g_j)]_{ij} \in M_{r\times r}(\mathbb{C}).$$

We remark that T is unique up to indices.

30.1 Character tables

Define

$$D = \begin{bmatrix} \#C_{g_1} & & 0 \\ & \ddots & \\ 0 & & \#C_{g_r} \end{bmatrix}.$$

Then the previous theorem gives the identity

$$\frac{1}{n} TDT^* = I.$$

Corollary 30.4 (Orthogonality II)**.** *For every $g, h \in G$,*

$$\sum_{i=1}^{r} \chi_{V_i}(g) \cdot \overline{\chi_{V_i}(h)} = \begin{cases} 0 & \text{if } g \text{ not conjugate to } h \\ \frac{n}{\#C_g} & \text{if } g, h \text{ are conjugate to each other.} \end{cases}$$

Proof. Because $n^{-1}TDT^* = I$, we get $DT^* = nT^{-1}$. Then $DT^*T = nI$ and $T^*T = nD^{-1}$. Taking the complex conjugation, we get $T^t\overline{T} = nD^{-1}$. □

Let us work out some examples.

	e	(12)	(123)
V_{triv}	1	1	1
V_{sign}	1	-1	1
$V_?$	2	0	-1

Table 2: Character table of S_3

Example 30.5. Take $G = S_3$ again. We have V_{triv} and V_{sign} that are 1-dimensional. A set of representatives for the conjugacy classes is $e, (12), (123)$. Using orthogonality, we can fill in the last row using orthogonality II with the first column.

After we have the character table, given any representation like permutation representation V_X, we know how many each representation is in it. $\chi_{V_X}(\sigma)$ is the number of fixed points of σ.

	e	(12)	(123)
V_X	3	1	0

Then we have

$$(\chi_X, \chi_{\text{triv}}) = \frac{1}{6}(3+3+0) = 1, \qquad (\chi_X, \chi_{\text{sign}}) = \frac{1}{6}(3-3+0) = 0,$$
$$(\chi_X, \chi_?) = \frac{1}{6}(6+0+0) = 0.$$

Therefore $V_X \cong V_{\text{triv}} \oplus V_?$.

Example 30.6. Take $G = S_4$. We again have V_{triv} and V_{sign}, and also V_{std}, which is defined as the kernel of the averaging operator of V_X, which has dimension $n-1$ in general and is irreducible. There are two more representations, and we can compute the dimensions, because the sum of their squares are 13, and so they have dimensions 2 and 3. But we still are not there to use orthogonality.

	e	(12)	$(12)(34)$	(123)	(1234)
V_{triv}	1	1	1	1	1
V_{sign}	1	-1	1	1	-1
V_{std}	3	1	-1	0	-1
V_3	3	-1	-1	0	1
V_2	2	0	2	-1	0

Table 3: Character table of S_4

Let us now try to make new characters from the ones we have. Try $V_{\text{sign}} \otimes V_{\text{std}} = W$. Then

	e	(12)	$(12)(34)$	(123)	(1234)
W	3	-1	-1	0	1

We can easily check whether W is irreducible, because

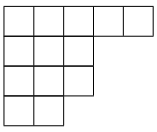
$$(\chi_W, \chi_W) = \frac{1}{24}(9 + 6 + 3 + 0 + 6) = 1.$$

So W is irreducible and $W = V_3$. Using orthogonality, we can get the last thing.

31 November 14, 2016

31.1 Constructing irreducible representations of S_m

Let $K = \mathbb{C}$ and $G = S_m$, and $n = \#G = m!$. In this case, $r = p(m)$ where $p(m)$ is the number of number of partitions. A **partition of** m is a tuple $\lambda = (\lambda_1, \dots, \lambda_k)$ such that $\sum \lambda_i = m$ and $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k$. For λ, the **diagram of** λ is

$\delta_\lambda =$ 

where the ith row has λ_i boxes. A more formal definition is, δ_λ is a suitable subset of $\{1, \dots, m\}^2$.

Definition 31.1. A **Young tableau** is a function $t : \delta_\lambda \to \{1, \dots, m\}$ which is bijective.

For example, the tableau

6	4	2
1	5	
7		
3		

is a tableau of shape $\lambda = (3, 2, 1, 1)$.

Definition 31.2. Let $X_\lambda = \{\text{tableaux of shape } \lambda\}$ for $t, s \in X_\lambda$, and for $t, s \in X_\lambda$, define $t \sim s$ if they have the same elements in each row. An equivalence class $[t]$ is called a **tabloid**. We write $\overline{X}_\lambda = \{\lambda - \text{tabloids}\}$.

There is a natural action of S_m on X_λ. And so S_m acts on $\overline{X}_\lambda$. Let $M^\lambda = (V_{\overline{X}_\lambda}, \rho_{\overline{X}_\lambda})$ be the permutation representation induced by this action. For example, if $\lambda = (m)$, then $\overline{X}_\lambda$ has one element, and so M^λ is the trivial representation. If $\lambda = (m-1, 1)$, then we get the permutation representation, which is $V_{\text{triv}} \oplus V_{\text{std}}$. Now here are our goals:

1. Construct the Specht module $S^\lambda \subseteq M^\lambda$.
2. Show that S^λ is irreducible.
3. Prove that $S^\lambda \cong S^\mu$ implies $\lambda = \mu$.

If we do this then we will be able to conclude that Specht modules are all irreducible representations of S_m.

Definition 31.3. For $t \in X_\lambda$, define $C_t \subseteq S$ as the column stabilizer of t. In other words, these are the permutations that move elements only within columns.

For instance,

$$t = \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 \\ \cline{1-1}\end{array} \quad \text{has} \quad C_t = \{\mathrm{id}, (13)\} \leq S_3.$$

Definition 31.4. For $t \in X_\lambda$ and $s \in X_\mu$, define the vectors:

$$E_{t,s} = \sum_{\sigma \in C_t} \epsilon(\sigma)\sigma \cdot e_{[s]} \in M^\mu.$$

This depends on t as a tableaux and s as a tabloid. We also write $E_t = E_{t,t}$.

Note that $\sigma E_t = E_{\sigma t}$, because $C_{\sigma t} = \sigma C_t \sigma^{-1}$.

Definition 31.5. We define the **Specht module** as

$$S^\lambda = \mathbb{C}\text{-span}\{E_t : t \in X_\lambda\} \subseteq M^\lambda.$$

Note that $S^\lambda = R \cdot E_{t_0}$ for any $t_0 \in X_\lambda$, because $\sigma E_t = E_{\sigma t}$ and G acts on the set of λ-tableaux transitively. So S^λ is a subrepresentation of M^λ. We cannot conclude that S^λ is irreducible only from the fact that it is generated by one vector.

31.2 Irreducibility of the Specht module

Definition 31.6. We write $\lambda \geq \mu$ if $\sum_{i \leq j} \lambda_i \geq \sum_{i \leq j} \mu_i$ for every j for which this makes sense.

For example, $(3,3,1,1) \geq (3,2,2,1)$. This is not a total order, but $\lambda \geq \mu$ and $\mu \geq \lambda$ implies $\lambda = \mu$.

Lemma 31.7. *Let λ, μ be partitions (of m). Suppose $t \in X_\lambda$ and $s \in X_\mu$ satisfying the condition that the entries on each row of s are in different columns of t. Then $\lambda \geq \mu$.*

This is an easy combinatorial exercise. For instance, take

$$t = \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 4 \\ \cline{1-1} 5 \\ \cline{1-1}\end{array}, \qquad s = \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 & 4 \\ \hline 5 \\ \cline{1-1}\end{array}.$$

This implies that $\lambda = (3,1,1) \geq \mu = (2,2,1)$. This is going to be used in showing that $S^\lambda \cong S^\mu$ implies $\lambda = \mu$.

Lemma 31.8. *Let $t \in X_\lambda$ and $s \in X_\mu$. Suppose $E_{t,s} \neq 0$. Then $\lambda \geq \mu$. If moreover $\lambda = \mu$, then $E_{t,s} = \pm E_t$.*

Proof. We assume $E_{t,s} \neq 0$. If there are $x \neq y$ in the same row of s and same column of t, then $(\mathrm{Id} - (xy))e_{[s]} = e_{[s]} - e_{[s]} = 0$. But $\langle \mathrm{Id}, (xy) \rangle \leq C_t$ because x and y lie in the same column. Let $\sigma_1, \ldots, \sigma_l$ be left coset representatives. Then

$$E_{t,s} = \sum_{j=1}^{l} \epsilon(\sigma_j)\sigma_j(\mathrm{Id} - (xy))e_{[s]} = 0.$$

This is a contradiction. Therefore each row of s, its elements are in different columns of t. Then Lemma 31.7 implies that $\lambda \geq \mu$.

Suppose that $\lambda = \mu$. Then from the condition that elements of each row of s are in different columns of t, we see that there exists a unique $\sigma_0 \in C_t$ such that $\sigma_0[t] = [s]$. So

$$\begin{aligned} E_{t,s} &= \sum_{\sigma \in C_t} \epsilon(\sigma)\sigma e_{[s]} = \sum_{\sigma \in C_t} \epsilon(\sigma)\sigma\sigma_0 e_{[t]} \\ &= \sum_{\sigma \in C_t} \epsilon(\sigma\sigma_0^{-1})\sigma e_{[t]} = \epsilon(\sigma_0)E_{t,t} = \pm E_t. \end{aligned}$$

□

32 November 16, 2016

For a tableau t, we defined a subgroup $C_t \leq S_m$, and we defined M^λ has the permutation representation of tabloids of shape λ. We also define the Specht module $S^\lambda \subseteq M^\lambda$, as generated by E_t for $t \in X_\lambda$. We had two lemmas: one about a combinatorial criterion for $\lambda \geq \mu$, and one about $E_{t,s} \neq 0$ implying $\lambda \geq \mu$.

Lemma 32.1. *Let $u \in M^\lambda$ and $t \in X_\lambda$. Then*

$$\left(\sum_{\sigma \in C_t} \epsilon(\sigma)\sigma\right) u \in \mathbb{C}E_t \in M^\lambda.$$

Proof. Write $u = \sum_{i=1}^{l} \alpha_i e_{[s_i]}$ for $\alpha_i \in \mathbb{C}$. Then

$$\left(\sum_{\sigma \in C_t} \epsilon(\sigma)\sigma\right) u = \sum_i \alpha_i E_{t,s_i} \in \mathbb{C}E_t$$

by Lemma 31.8. □

This operator seems interesting, so define

$$\pi_t = \sum_{\sigma \in C_t} \epsilon(\sigma)\sigma \in R.$$

Definition 32.2. Define the inner product $\langle \bullet, \bullet \rangle_\lambda$ on M^λ by

$$\langle e_{[s]}, e_{[t]} \rangle_\lambda = \begin{cases} 1 & \text{if } [s] = [t] \\ 0 & \text{otherwise.} \end{cases}$$

Proposition 32.3. *π_t is self-adjoint with respect to the inner product $\langle \bullet, \bullet \rangle_\lambda$.*

Proof. We have

$$\begin{aligned} \langle \pi_t u, v \rangle &= \sum_{\sigma \in C_t} \epsilon(\sigma) \langle \sigma u, v \rangle = \sum_{\sigma \in C_t} \epsilon(\sigma) \langle u, \sigma^{-1} v \rangle \\ &= \sum_{\tau \in C_t} \epsilon(\tau^{-1}) \langle u, \tau v \rangle = \langle u, \pi_t v \rangle. \end{aligned}$$

□

Lemma 32.4 (Submodule theorem)**.** *Let $W \subseteq M^\lambda$ be a subrepresentation. Then W contains S^λ or W is orthogonal to S^λ. In particular, S^λ is irreducible.*

Proof. Let $u \in W$ and $t \in X_\lambda$. Lemma 32.1 implies that $\pi_t v = \alpha_{u,t} E_t$ for $\alpha_{u,t} \in \mathbb{C}$.

Case 1: for some $u_0 \in W$ and $t_0 \in X_\lambda$, we have $\alpha_0 = \alpha_{u_0,t_0} \neq 0$.
Because $u_0 \in W$, we also have $\pi_t u_0 \in W$ and so $E_{t_0} = \alpha_0^{-1} \pi_t u \in W$. Because S^λ is generated by any E_{t_0} as an R-module, it follows that $S^\lambda = R \cdot E_{t_0} = W$.

Case 2: for every $u \in W$ and every $t \in X_\lambda$, we have $\alpha_{0,t} = 0$.
In other words, $\pi_t u = 0$. Let $[s]$ be any tabloid. Then

$$0 = \langle 0, e_{[s]} \rangle = \langle \pi_t u, e_{[s]} \rangle = \langle u, \pi_t e_{[s]} \rangle = \langle u, E_{t,s} \rangle.$$

Thus letting $s = t$, S^λ and W are orthogonal. □

32.1 Specht modules are all the irreducible representations

Lemma 32.5. *Let $f \in \mathrm{Hom}_G(M^\lambda, M^\mu)$. Suppose $S^\lambda \not\subseteq \ker f$. Then $\lambda \geq \mu$.*

Proof. By Lemma 32.4, we see that S^λ is orthogonal to $\ker f$. For every $t \in X_\lambda$, E_t is orthogonal to $\ker f$. So

$$0 \neq f(E_t) = f\pi_t e_{[t]} = \pi_t f e_{[t]}$$

because $E_t \neq 0$ and $f e_{[t]} = \sum \alpha_i e_{[s_i]}$ for $s_i \in X_\mu$. So $0 \neq \pi_t \sum \alpha_i e_{[s_i]} = \sum \alpha_i E_{t,s_i}$. This implies that there exists a $t \in X_\lambda$ and $s \in X_\mu$ with $E_{t,s} \neq 0$. Then by Lemma 31.8, $\lambda \geq \mu$. □

Lemma 32.6. *Let $f \in \mathrm{Hom}_G(S^\lambda, S^\mu)$. If $f \neq 0$, then $\lambda \geq \mu$.*

Proof. Extend f to a $\mathbb{C}$-linear map $\tilde{f} : M^\lambda \to S^\mu \subseteq M^\mu$ by 0 on $(S^\lambda)^\perp$. Then $\tilde{f}$ is R-linear. (You can directly check this.) Then Lemma 32.5 shows that $\lambda \geq \mu$. □

Theorem 32.7. *The Specht modules S^λ for λ a partition of m give the full list (with no repetitions) of irreducible representations of S_m.*

32.2 Restricted representation

I am going to take $H \leq G$ and $R_G = \mathbb{C}[G]$ and $R_H = \mathbb{C}[H]$. Then we have a natural inclusion $R_H \subseteq R_G$. Therefore the restriction of scalars give a functor

$$\mathrm{Res}^G_H : {}_G\mathsf{Rep} \to {}_H\mathsf{Rep}; \quad (V, \rho) \mapsto (V, \rho|_H).$$

This is functorial, because there is a map

$$\mathrm{Hom}_G(V, W) \to \mathrm{Hom}_H(\mathrm{Res}\, V, \mathrm{Res}\, W); \quad f \mapsto f.$$

Recall that if $A \to B$ is an commutative algebra and M an A-module and N a B-module, then what we are doing is restriction of scalars $\mathrm{Res} : N \mapsto {}_A N$. But this has an adjoint, which is extension by scalars:

$$T : M \mapsto M_B = B \otimes_A M.$$

That is, there is an A-linear isomorphism

$$\mathrm{Hom}_B(B \otimes_A M, N) \cong \mathrm{Hom}_A(M, {}_A N).$$

The analogue for this is going to be the induced representation.

33 November 18, 2016

Last time we saw that if $H \leq G$, then there is a canonical inclusion $R_H \hookrightarrow R_G$ and so there is a restriction functor Res^G_H given by restriction of scalars. To define the adjoint operation, we need some notion of tensor product.

33.1 Tensor products for non-commutative rings

Let R be a ring, which is not necessarily commutative. Let M be a right R-module and N be a left R-module. A **balanced map** is a map $b : M \times N \to X$ with:

(1) X is an abelian group,

(2) b is bi-additive,

(3) $b(mr, n) = b(m, rn)$.

We then define the **tensor product** $M \otimes_R N$ as the universal balanced map $\tau : M \times N \to M \otimes_R N$. This exists, because we can construct it as

$$M \otimes_R N = \frac{\langle m \otimes n : m \in M, n \in N \rangle_{\mathbb{Z}\text{-Mod}}}{\langle \text{relations} \rangle}.$$

If $f : \mathrm{Hom}_{\mathsf{Mod}_R}(M, M')$ and $g \in \mathrm{Hom}_{{}_R\mathsf{Mod}}(N, N')$, we get a map $f \otimes g : M \otimes_R N \to M' \otimes_R N'$.

$$\begin{array}{ccc} M \times N & \xrightarrow{f \times g} & M' \times N' \\ \downarrow & \overset{\text{bal.}}{\searrow} & \downarrow \\ M \otimes_R N & \xrightarrow{f \otimes g} & M' \otimes_R N' \end{array}$$

Let M be a (R', R)**-bimodule**, i.e.,

(1) M is a left R'-module,

(2) M is a right R-module,

(3) $(r'm)r = r'(mr)$.

Then for every $r' \in R'$, the multiplication map $\mu_{r'}$ is in $\mathrm{Hom}_{\mathsf{Mod}_R}(M, M')$. So there is a natural left R'-module structure on $M \otimes_R N$.

Consider the special case when R' is an R-algebra, i.e., $R \to R'$. Then R' is a (R', R)-bimodule. So we get a functor

$$ {}_R\mathsf{Mod} \to {}_{R'}\mathsf{Mod}; \quad N \mapsto R' \otimes_R N.$$

Further note that there is a natural isomorphism

$$\mathrm{Hom}_{R'}(R' \otimes_R M, N) \cong \mathrm{Hom}_R(M, {}_R N)$$

where M is a left R-module and N is a left R'-module.

33.2 Induced representation

Definition 33.1. We define the **induced representation functor**

$$\mathrm{Ind}_H^G : {}_H\mathsf{Rep} \to {}_G\mathsf{Rep}; \quad V \mapsto \mathrm{Ind}_H^G(V) = R_G \otimes_{R_H} V.$$

There is a more concrete definition of the induced representation, which is good for computation. Define $\mathrm{Ind}_H^G V = \bigoplus_{i=1}^{l} g_i V$ where:

(1) $g_1, \ldots, g_l$ are left coset representatives for G/H so that $G = \bigcup g_i H$,

(2) $g_i V$ are $\mathbb{C}$-isomorphic copies of V with the formal isomorphisms $V \cong g_i V$ with $g \mapsto g_i x$,

(3) $g \cdot g_i x = g_j h x$ where j, h depends on g, i as follows: $g g_i \in G$ so we let $g g_i = g_j h$.

Example 33.2. Take $H = \langle 1 \rangle \leq G$. Then $\mathrm{Ind}\, V_{\mathrm{triv},H} = V_{\mathrm{reg},G}$. We can see this from $R_G \otimes_{R_H} \mathbb{C} \cong R_G$. Alternatively, you can look at the concrete construction. Because H has one element, $g_1, \ldots, g_l$ has to have all elements G and the action must be the same thing as the action on the representation because $g \cdot g_i = (g g_i) \cdot 1_H$.

Proposition 33.3 (Frobenius reciprocity)**.** *For V a H-representation and W a G-representation,*

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

Thus, $(\chi_{\mathrm{Ind}\, V}, \chi_W)_G = (\chi_V, \chi_{\mathrm{Res}\, W})_H$.

These stuff are used in number theory. In the proof of the infinitude the primes in an arithmetic progression, Dirichlet used the twisted Riemann zeta function, with characters 1-dimensional representations in the denominator. Then other people started to consider more general representation and Hecke developed a full theory of this and Artin proved some theorem about representations coming from induced representation.

33.3 Characters of restricted and induced representation

Clearly $\chi_{\mathrm{Res}\, V} = \mathrm{Tr}(\rho_V|_H) = \chi_V|_H$. For the induced representation, we can use the concrete definition of Ind and realize g as a huge block matrix. Then

$$\begin{aligned}\chi_{\mathrm{Ind}\, V}(g) &= \sum_{g : g_i V \to g_i V} \mathrm{Tr}(g | g_i V) = \sum_{g_i^{-1} g g_i \in H} \mathrm{Tr}(g_i^{-1} g g_i | V) \\ &= \frac{1}{\#H} \sum_{\substack{g_0 \in G \\ g_0^{-1} g g_0 \in H}} \mathrm{Tr}(g_0^{-1} g g_0 | V) = \frac{1}{\#H} \sum_{\substack{g_0 \in G \\ g_0^{-1} g g_0 \in H}} \chi_V(g_0^{-1} g g_0).\end{aligned}$$

Denote

$$\Omega_H = \mathbb{C}\text{-class functions on } H, \quad \Omega_G = \mathbb{C}\text{-class functions on } G,$$

and also let

$$\Lambda_H = \mathbb{Z}\text{-linear combinations of } G\text{-representations}$$

and likewise Λ_G. Then $\Lambda_H \subseteq \Omega_H$ and $\Lambda_G \subseteq \Omega_G$. Also the definition of induced and restricted representations gives maps $\mathrm{Res} : \Lambda_G \to \Lambda_H$ and $\mathrm{Ind} : \Lambda_H \to \Lambda_G$.

34 November 21, 2016

We have a map $\mathrm{Ind} : \Omega_H \to \Omega_G$ given by

$$\psi(-) \mapsto \frac{1}{\#H} \sum_{\substack{g_0 \in G \\ g_0^{-1}(-)g_0 \in H}} \psi(g_0^{-1}(-)g_0).$$

By definition, $\mathrm{Ind}(\Lambda_H) \subseteq \Lambda_G$. Likewise, we have restriction maps $\mathrm{Res} : \Omega_G \to \Omega_H$ and $\mathrm{Res}(\Lambda_G) \subseteq \Lambda_H$.

34.1 Artin induction theorem

Lemma 34.1. *Λ_G and Λ_H are commutative unitary rings.*

Proof. We only need to check that Λ_G and Λ_H are closed under multiplication. To do this, use the tensor product. □

Lemma 34.2. Res *is a ring morphism and* Ind *is a group morphism.*

Proof. This is clear. □

Lemma 34.3. *$\mathrm{Ind}(\Lambda_H) \subseteq \Lambda_G$ is an ideal.*

Proof. The image is clearly closed under addition. Let $\psi \in \Lambda_H$ and $\xi \in \Lambda_G$. We want to show that $\mathrm{Ind}(\psi) \cdot \xi$ is in $\mathrm{Ind}(\Lambda_H)$. Let $g \in G$. Then

$$\begin{aligned}((\mathrm{Ind}\,\psi) \cdot \xi)(g) &= \frac{1}{\#H} \sum_{\substack{g_0 \in G \\ g_0^{-1} g g_0 \in H}} \psi(g_0^{-1} g g_0)\xi(g) \\ &= \frac{1}{\#H} \sum_{\substack{g_0 \in G \\ g_0^{-1} g g_0 \in H}} \psi(g_0^{-1} g g_0)\xi(g_0^{-1} g g_0) = \mathrm{Ind}(\psi \cdot \mathrm{Res}(\xi))(g).\end{aligned}$$

So we have $(\mathrm{Ind}\,\psi) \cdot \xi = \mathrm{Ind}(\psi \cdot \mathrm{Res}(\xi))$. □

The image has no reason to be the whole ring. But we will soon see that it is close to being the whole ring. In fact, a suitable multiple of 1 is in the image, so it is a full sub-lattice.

Definition 34.4. If K is a cyclic group, define the "special" character $\xi_K \in \Omega_K$ by:

$$\xi_K(k) = \begin{cases} \#K & \text{if } \langle k \rangle = K \\ 0 & \text{otherwise.} \end{cases}$$

Let us denote by $\mathrm{Cyc}(G)$ the set of cyclic groups of G. We remark that

$$\sum_{H\in\mathrm{Cyc}(G)} \mathrm{Ind}_H^G(\xi_H)(g) = \sum_{H\in\mathrm{Cyc}(G)} \frac{1}{\#H} \sum_{\substack{g_0\in G \\ g_0^{-1}gg_0\in H}} \chi_H(g_0^{-1}gg_0)$$
$$= \sum_{H\in\mathrm{Cyc}(G)} \sum_{\langle g_0^{-1}gg_0\rangle = H} 1 = \#G.$$

This looks very promising.

Lemma 34.5. *It H is cyclic,then $\xi_H \in \Lambda_H$.*

Proof. We proceed by induction on $\#H$. It is clear if $\#H = 1$. For the inductive step, we use the remark. We have

$$\sum_{K\in\mathrm{Cyc}(H)} \mathrm{Ind}_K^H(\xi_K) = \#H.$$

So $\xi_H = \# \cdot \xi_{\mathrm{triv}} -$ (some representations). This shows that $\xi_H \in \Lambda_H$. □

Theorem 34.6 (Artin)**.** *Let V be a G-representation. Then ξ_V is a $\mathbb{Q}$-linear combination of characters induced from cyclic subgroups of G.*

Proof. We have

$$I_G = \sum_{H\in\mathrm{Cyc}(G)} \mathrm{Ind}_H^G(\Lambda_H) \subseteq \Lambda_G$$

as an ideal. By the remark, the constant function $\#G \cdot \xi_{\mathrm{triv}}$ is in I_G. Therefore $(\#G) \cdot \chi_V \in I_G$. □

Brauer showed a more stronger theorem, by allowing groups that are called elementary subgroups, but restricting to integer linear combinations.

34.2 Connections to analytic number theory

In 1737, Euler defined

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

for $s > 1$, and noted that this diverges as $s \to 1+$. He figured out that you can factor it as

$$\zeta(s) = \prod_p \Big(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\Big) = \prod_p \Big(1 - \frac{1}{p^s}\Big)^{-1}.$$

So there has to infinitely many primes, for analytic reasons. Even now, this is the best way to count primes.

Around 1837–1838, Dirichlet proved the fact that there are infinitely many primes in any congruence class $p \equiv a \pmod{N}$ for $(a, N) = 1$. Here is Dirichlet's amazing approach. Take $G = (\mathbb{Z}/N\mathbb{Z})^\times$, which is abelian. For $\chi : G \to \mathbb{C}^\times$, he defined

$$L(s, \chi) = \sum_{(n,N)=1} \frac{\chi(n)}{n^s} = \prod_{p \nmid n} \Big(1 - \frac{\chi(p)}{p^s}\Big)^{-1}$$

again by unique factorization, for $s > 1$. Then using the fact that $\chi(p)/p^s$ is small, we can write

$$\log L(s, \chi) = \sum_{p \nmid N} -\log\Big(1 - \frac{\chi(p)}{p^s}\Big) = \sum_{p \nmid N} \sum_{r=1}^{\infty} \frac{1}{r} \frac{\chi(p^r)}{p^{rs}} = \sum_{p \nmid N} \frac{\chi(p)}{p^s} + g_\chi(s),$$

where $|g_\chi(s)| < C$ independent of χ and N. Using orthogonality, we can say

$$\begin{aligned} F_{N,a}(s) &= \frac{1}{\varphi(N)} \sum_\chi \overline{\chi(a)} \log L(s, \chi) = \frac{1}{\phi(N)} \sum_\chi \sum_{p \nmid N} \frac{\chi(p)\overline{\chi(a)}}{p^s} + b_N(s) \\ &= \sum_{p \equiv a \pmod{N}} \frac{1}{p^s} + b_N(s) \end{aligned}$$

where b_N is uniformly bounded. So the goal is to show that $F_{N,a}(s) \to \infty$ as $s \to 1^+$.

There are basically two cases. If $\chi = \chi_{\text{triv}}$ then $L(s, \chi_{\text{trvi}})$ is $\sum_{(n,N)=1} 1/n^s$ and this diverges. If $\chi \neq \chi_{\text{triv}}$, you can show that $L(1, \chi) \neq 0, \infty$.

35 November 28, 2016

35.1 Lie groups

Definition 35.1. A **Lie group** is a group $(G, 1, \cdot)$ satisfying:

(1) G is a C^∞ $\mathbb{R}$-manifold,

(2) the multiplication map $\cdot : G \times G \to G$ is C^∞,

(3) the inversion map $i : G \to G; x \mapsto x^{-1}$ is C^∞.

A morphism between Lie groups is a group morphism which is C^∞.

Clearly $\mathbb{R}$ and $\mathbb{C}$ with addition are Lie groups. Also $\mathbb{R}^\times$ and $\mathbb{C}^\times$ with $\cdot$ are Lie groups. The circle $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ with multiplication is also a Lie group. This is isomorphic to $\mathbb{R}/\mathbb{Z}$ with addition. More generally, $\mathbb{R}^n/\Lambda$ with addition is a Lie group, where Λ is a lattice.

More interesting examples are $\mathrm{GL}_n(\mathbb{R})$ and $\mathrm{GL}_n(\mathbb{C})$ with multiplication. Likewise $\mathrm{SL}_n(\mathbb{R})$ and $\mathrm{SL}_n(\mathbb{C})$ are Lie groups. The group $\mathrm{B}(n)$ of upper triangular matrices over $\mathbb{R}$ and B_n of upper triangular matrices over $\mathbb{C}$ with multiplication are Lie groups. There is a confusion convention that real Lie groups have n in the parentheses and complex Lie groups have n in the subscript. We also define

$$\mathrm{O}(n) = \{A \in \mathrm{GL}_n(\mathbb{R}) : A^t A = I\},$$
$$\mathrm{U}(n) = \{A \in \mathrm{GL}_n(\mathbb{C}) : A^* A = I\}.$$

Note that $\mathrm{U}(n)$ is *not* a complex manifold, because the condition is not holomorphic. We have $\mathrm{SO}(n)$ and $\mathrm{SU}(n)$, which are $\mathrm{O}(n)$ and $\mathrm{U}(n)$ that have determinant 1.

We have an isomorphism $\mathbb{R} \cong B(2)$. Note that this is precisely the counterexample we saw when talking about irreducible representations being simple.

Definition 35.2. A **representation** of a Lie group G is a pair (V, ρ) with

(1) V a finite dimensional $\mathbb{C}$-vector space,

(2) $\rho : G \to \mathrm{GL}_{\mathbb{C}}(V)$ is a morphism of Lie groups.

For example,

$$\rho : \mathbb{R} \to \mathrm{GL}_2(\mathbb{C}); \quad x \mapsto \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$$

is *not* semi-simple.

So we start to panic. But we can make this through. The key feature of the theory of Lie groups are linearization of two kinds: of representations and of Lie algebras.

35.2 The Haar measure and averaging

What went wrong with the map $\mathbb{R} \to \mathrm{GL}_2(\mathbb{C})$? The whole point of Maschke's theorem was the averaging operator. But in this case, groups are infinite. So we would like integrate instead of adding elements.

Theorem 35.3 (In Knaap, Ch. VIII)**.** *Let G be a Lie group. There is a Borel measure μ on G which is left-invariant, i.e.,*

$$\int_G \psi(g)d\mu(g) = \int_G \psi(hg)d\mu(g).$$

Such a μ is unique up to scalar. If G is compact then μ is unique if we require that it is a probability measure (i.e., $\int_G d\mu(g) = 1$). Furthermore, μ is bi-invariant. This μ is called the ***Haar measure****.*

Example 35.4. Take $\mathbb{R}/\mathbb{Z}$ with the Lebesgue measure. This is the Haar measure. If G is finite, then the measure

$$\mu = \frac{1}{\#G}\sum_{g\in G} f_g$$

is the Haar measure.

Assume G is compact. Let (V, ρ) be a representation. Define the averaging operator

$$\mathrm{Avg}_V : V \to V^G; \quad x \mapsto \int_G \rho(g)(x)d\mu(g).$$

Lemma 35.5. *If (V, ρ) is a representation, then ρ is unitary for a certain $\langle\ ,\ \rangle_\rho$ on V.*

Proof. Let $\langle\ ,\ \rangle$ be any inner product in V. Define

$$\langle x, y\rangle_\rho = \int_G \langle\rho(g)x, \rho(g)y\rangle d\mu(g).$$

Check that it works. □

Theorem 35.6 (Weyl)**.** *Let G be a compact Lie group.*

(1) [easy] All finite dimensional $\mathbb{C}$-linear representations of the Lie group G are semi-simple.

(2) [requires some analysis] The set $\{\chi_V : V \text{ irred.}\}$ is an orthonormal Hilbert basis for Ω. In particular, they are countable. Here,

$$\Omega = L^2(G, \mu)_{\mathbb{C}}^{G\text{-}conj.}, \quad (\psi, \xi)_\Omega = \int_G \psi(g)\overline{\xi(g)}d\mu(g).$$

36 November 30, 2016

Let G be a compact Lie group. We have the space $\Omega = L^2(G,\mu)^{\text{conj}}_{\mathbb{C}}$ that is a Hilbert space under the inner product $\int_G \psi(g)\overline{\xi(g)}d\mu(g)$. Then our theorem will say that $\{\chi_V : V \text{ irreducible}\}$ is a Hilbert basis of Ω.

36.1 Irreducible representations of S^1

Let us look at an example first. The simplest compact Lie group is $U(1) = S^1 \cong \mathbb{R}/\mathbb{Z}$. Then μ is just the Lebesgue measure. Because the group is abelian, we have $\Omega = L^2([0,1], \text{Leb})$. We claim that if V is an irreducible representation, then $\dim V = 1$. If (V,ρ) is irreducible, then $\rho|_{\langle 1/n\rangle} = \rho_n : C_n \to \text{GL}(V)$ is a representation of a cyclic group. Note that the sets $\langle 1/n\rangle$ equidistributes in $(\mathbb{R}/\mathbb{Z}, \text{Leb})$. This is saying that

$$\frac{1}{n}\sum_{j=1}\delta_{j/n} \xrightarrow{w^*} \text{Leb}$$

as $n \to \infty$. Then we get

$$\lim_{n\to\infty}\int_{\langle 1/n\rangle}|\chi_{\rho_n}|^2 d\text{Dirac} = \int_G |\chi_\rho|^2 d\text{Leb} = 1$$

because χ is irreducible. But the sum $\int_{\langle 1/n\rangle}|\chi_{\rho_n}|^2 d\text{Dirac}$ is an integer. This shows that for $n \gg 1$, ρ_n is irreducible.

Proposition 36.1. *The only irreducible representations of $G = \mathbb{R}/\mathbb{Z}$ are: for $n \in \mathbb{Z}$, $e_n : \theta \mapsto e^{2\pi i n\theta} \in \text{GL}_1(\mathbb{C})$. This can also be written as $e_n = e_1^{\otimes n}$ with $e_1^{\otimes -1} = e_1^\vee$.*

Proof. First note that the e_n's are distinct irreducible representations. Let (V,ρ) be an irreducible representation. Then $\dim V = 1$ and ρ is unitary. So $\rho : G \to S^1$.

Take $\rho(\theta) = \exp(2\pi i f(\theta))$ where $f : \mathbb{R} \to \mathbb{R}$ is the lifting to the universal covering. Then $f(t) = \alpha t$ for some $\alpha \in \mathbb{R}$. Going back to S^1, we figure out that α has to be an integer. □

Corollary 36.2. *The functions $e_n(\theta) = e^{2\pi i n\theta}$ for $n \in \mathbb{Z}$ form an orthonormal Hilbert basis for $L^2([0,1], \text{Leb})$.*

This recovers the Fourier theory for L^2 spaces.

36.2 The tangent space

Let M be a C^∞ manifold in general, with $n = \dim M \geq 1$.

Definition 36.3. For a point $p \in M$, a **curve at** p is a map $\gamma : (-\epsilon, \epsilon) \to M$, smooth, with $\gamma(0) = p$.

We say that $\gamma_1 \sim \gamma_2$ if for every $f \in C^\infty U$ with small enough $U \ni p$, $(f \circ \gamma_1)'(0) = (f \circ \gamma_2)'(0)$. Define the **tangent space** as

$$T_pM = \{[\gamma] : \gamma \text{ a curve at } p\}.$$

So far this is a pointed set with the point being $[\text{const}_p]$.

Let $\varphi : U \to \mathbb{R}^n$ be a chart at p. Define

$$\Psi_\varphi : T_pM \to \mathbb{R}^n; \quad [\gamma] \mapsto (((\pi_i \circ \varphi) \circ \gamma)'(0))_{i=1}^n.$$

It is an exercise that Φ_φ is bijective. Furthermore, given two different charts φ_1, φ_2, we have $\Psi_{\varphi_1} \circ \Psi_{\varphi_2}^{-1} \in \text{GL}_n(\mathbb{R})$. Also $[\text{const}_p] \mapsto 0$ by Ψ_φ.

Corollary 36.4. *T_pM has a unique $\mathbb{R}$-vector space structure such that $[\text{const}_p] = 0$ and for every chart φ at p, Ψ_φ is a linear isomorphism.*

Definition 36.5. The **differential** is a functor

$$d : \mathsf{pointedManifolds} \to \mathbb{R}\text{−}\mathsf{vsp}; \quad d(M,p) = T_pM,$$

with morphisms given by

$$F \in \text{Mor}((M,p),(N,q)) \quad \mapsto \quad (d_pF : T_pM \to T_q;\ [\gamma] \mapsto [F \circ \gamma]).$$

Definition 36.6. A **vector field** is a function $X : C^\infty M \to C^\infty M$ satisfying

(D1) X is $\mathbb{R}$-linear,

(D2) for every $f, g \in C^\infty M$, $X(f \cdot g) = X(f) \cdot g + f \cdot X(g)$.

For example, if $M = U \subseteq \mathbb{R}^n$, then all the vector fields are of the form

$$X = \sum_{i=1}^n h_i \frac{\partial}{\partial x_i}$$

for $h_i \in C^\infty U$.

Definition 36.7. The **tangent bundle** TM is the $C^\infty M$-module of vector fields on M.

Given a point $p \in M$ and a vector field $X \in TM$, we can get a $X_p \in TM$. There are two ways of getting this. We can argue that there exists a curve γ at p such that for all $f \in C^\infty M$, $X(f)(p) = (f \circ \gamma)'(0)$. This γ is not unique, but $[\gamma]$ is uniquely defined. So $X_p = [\gamma]$ is well-defined. Another constructive way of doing this (in the local case) is to first write $X = \sum h_i(\partial/\partial x_i)$ and define $X_p = \Psi_{\text{Id}_U}^{-1}((h_i(p))_{i=1}^m)$. These two give the same answer.

Lemma 36.8. *The function $\tau_X : M \to \coprod_{p \in M} T_pM$ defined by $p \mapsto X_p$ determines X uniquely.*

Proof. $X \mapsto \tau_X$ is $\mathbb{R}$-linear. If $\tau_X(p) \equiv 0$ then $X_p = 0$ for every p, and then $X(f)(p) = (f \circ \text{const})'(0) = 0$. This means that $X(f) = 0$ for every $f \in C^\infty M$. That is, $X = 0$. □

Define for $F : M \to N$ the map $dF : TM \to TN;\ X \mapsto X \circ F^*$. Then

$$((dF)(X))_{F(p)} = (d_pF)(X_p).$$

37 December 2, 2016

Last time, for a n-manifold M, we defined the tangent space T_pM at p. We also define TM, which is the $C^\infty M$-module of vector fields. Here, $\{X_p\}_{p\in M}$ uniquely determines X.

37.1 Left-invariant vector fields of Lie groups

Let $(G; e, \cdot)$ be a Lie group and let $n = \dim G \geq 1$.

Definition 37.1. Given $g \in G$, define $L_g : G \to G$ as $p \mapsto g \cdot p$. This induces a map $L_g^* : C^\infty G \to C^\infty G$ given by $L_g^*(f)(p) = f(g \cdot p)$. We say that $X \in TM$ is **left-invariant** if for every $g \in G$, $L_g^* \circ X = X \circ L_g^*$.

Equivalently, we can say this as for every group element $g \in G$ and a point $p \in G$,

$$(d_pL_g)X_p = X_{g\cdot p}.$$

For example, if $G = \mathbb{R}$, then the invariant vector fields will be $X = d/dt$ up to scalar multiplication. Then $f'(t+\alpha)$ and $(f(t+\alpha))'$ are the same. Let us look at a more interesting example. Let $G = \mathbb{R}_{>0}$ with multiplication. Then $X = t(d/dt)$ is an invariant vector field. The commutation of L_g^* and X can be checked as

$$\begin{aligned}(L_g^* \circ X)(f) &= L_g^*(tf'(t)) = (tg)f'(tg),\\ (X \circ L_g^*)(f) &= X(f(g\cdot t)) = t\frac{d}{dt}f(gt) = tgf'(gt).\end{aligned}$$

Definition 37.2. Define LTG the $\mathbb{R}$-vector space of left-invariant vector fields of G.

Proposition 37.3. *The map $LTG \to T_eG$ given by $X \mapsto X_e$ is an isomorphism of $\mathbb{R}$-vector spaces. The inverse is determined by*

$$v \in T_eG \quad \mapsto \quad X^v \text{ the only } X \text{ such that for all } p,\ (d_eL_p)(v) = X_p.$$

The only thing you need to check is that X_p defined as in the proposition varies in a C^∞ way. This can be done locally.

Definition 37.4. We define $\mathrm{Lie}(G) = \mathfrak{g} = T_eG \cong LTG$.

Definition 37.5. Let $X \in TM$. An **integral curve** for X is a C^∞ function $\gamma : I^0 \to M$ such that for all $t_0 \in I^0$, $[\gamma(t+t_0)] = X_{\gamma(t_0)}$.

Proposition 37.6. *Let $X \in LTG$ and let $X \neq 0$. Then there is a unique* global *integral curve $\gamma : \mathbb{R} \to G$ for X satisfying $\gamma(0) = e$.*

It turns out that $\gamma(s_0 + t_0) = \gamma(s_0) \cdot \gamma(t_0)$. That is, the group is abelian along this curve. The idea of the proof is to define another curve $\tilde{\gamma}(t) = \gamma(s_0)^{-1} \cdot \gamma(s_0 + t)$. The by uniqueness, $\tilde{\gamma} = \gamma$.

In our previous example $G = \mathbb{R}_{>0}$ and $X = t(d/dt)$, the integral curve for X is $\gamma(t) = e^t$. This is because $\gamma(0) = 1$ and $(f \circ \gamma)'(t_0) = f(e^t)'|_{t_0} = e^{t_0} f'(e^{t_0})$ and $X(f)(\gamma(t_0)) = tf'(t)|_{e^{t_0}} = e^{t_0} f'(e^{t_0})$.

Definition 37.7. A **1-parameter subgroup** is a morphism $\gamma : \mathbb{R} \to G$ of Lie groups.

So far, from a vector $v \in \mathfrak{g}$, we have obtained a left-invariant vector field X^γ and then a 1-parameter subgroup $\gamma_v : \mathbb{R} \to G$. Given γ_v, it is not hard to recover v. It is just $[\gamma_v] = v \in \mathfrak{g}$.

37.2 The exponential map

Definition 37.8. The **exponential map** $\exp : \mathfrak{g} \to G$ is defined by $v \mapsto \gamma_v(1)$.

In the example $G = \mathbb{R}_{>0}$, a vector $\lambda \in \mathbb{R} = T_1 G$ gives a left-invariant vector field $X_\lambda = \lambda t(d/dt)$. Then we get the curve $\gamma_\lambda(t) = e^{\lambda t}$. So $\exp_G(\lambda) = e^\lambda$.

The reason we care about this map is because it allows us to go back from morphisms of the tangent space to the morphisms of Lie groups.

Theorem 37.9. *Let G, H be Lie groups and suppose that G is connected. Then the map*

$$d : \mathrm{Mor}_{\mathsf{LieGrp}}(G, H) \to \mathrm{Mor}_{\mathbb{R}-\mathsf{vsp}}(\mathfrak{g}, \mathfrak{h})$$

is injective.

The reason this is true is because the diagram

$$\begin{array}{ccc} \mathfrak{g} & \xrightarrow{dF} & \mathfrak{h} \\ {\scriptstyle \exp_G}\downarrow & & \downarrow{\scriptstyle \exp_H} \\ G & \xrightarrow{F} & H \end{array}$$

that commutes. Because exp is a diffeomorphism near $0 \mapsto e$, dF determines F locally, and then determines the whole map F locally.

If you have two $X, Y \in TM$, then they are maps $C^\infty M \to C^\infty M$. In general, $X \circ Y$ doesn't satisfy the Leibniz rule, but $X \circ Y - Y \circ X$ does. So we can define

$$[X, Y] = X \circ Y - Y \circ X \in TM.$$

It is also true that if X and Y are left-invariant, then $[X, Y]$ is also left-invariant. Thus $\mathfrak{g}$ also have this $[\ ,\ ]$. This bracket satisfies some relations.

(1) $[\ ,\ ]$ is $\mathbb{R}$-bilinear.

(2) It is alternating, i.e., $[X, X] = 0$.

(3) The Jacobi formula

$$[X,[Y,Z]]+[Y,[Z,X]]+[Z,[X,Y]]=0$$

holds.

Definition 37.10. A $\mathbb{R}$-vector space with such an operation $[\ ,\ ]$ is called a **Lie algebra** over $\mathbb{R}$.

Theorem 37.11. *Let G, H be Lie groups. Suppose G is simply connected. Then*

$$d : \mathrm{Mor}_{\mathsf{LieGrp}}(G,H) \to \mathrm{Mor}_{\mathbb{R}-\mathsf{LieAlg}}(\mathfrak{g},\mathfrak{h})$$

is bijective.

Index