Math 552: Abstract Algebra II

Wolmer V. Vasconcelos

Set 3

Spring 2009

Outline

Rings in L.A.

Several modules over rings occur in Linear Algebra. We will develop the theory of finitely generated modules over certain rings and apply it to L.A.

Example

Let $\mathbf{V}$ be a finite dimensional vector space over the field k, and let

$$\varphi : \mathbf{V} \longrightarrow \mathbf{V}$$

be a linear transformation. Define a $k[\mathbf{x}]$-module structure $\mathbf{M}$ by declaring

$$x \cdot v = \varphi(v), \quad \forall v \in \mathbf{V}.$$

More generally, for a polynomial $\mathbf{f}(\mathbf{x})$, define

$$\mathbf{f}(\mathbf{x})v = \mathbf{f}(\varphi)(v).$$

We denote this module by $\mathbf{V}_\varphi$. If ϕ is another linear transformation of $\mathbf{V}$, similarly we get a module $\mathbf{V}_\phi$.

Although $\mathbf{V}_\varphi$ and $\mathbf{V}_\phi$ are the same vector space, as $k[\mathbf{x}]$-modules they may not be isomorphic.

Proposition

Let $\mathbf{A}$ *and* $\mathbf{B}$ *be* $n \times n$ *matrices over* k *and denote by* $\mathbf{V_A}$ *and* $\mathbf{V_B}$ *the corresponding* $k[\mathbf{x}]$*-modules defined on* $\mathbf{V} = k^n$*. Then* $\mathbf{V_A}$ *and* $\mathbf{V_B}$ *are isomorphic* $k[\mathbf{x}]$*-modules iff* $\mathbf{A}$ *and* $\mathbf{B}$ *are similar, that is if there is an invertible matrix* $\mathbf{S}$ *such that* $\mathbf{A} = \mathbf{S}^{-1}\mathbf{B}\mathbf{S}$*.*

Proof. If $\mathbf{S} : \mathbf{V_A} \simeq \mathbf{V_B}$ is an isomorphism of $k[\mathbf{x}]$-modules, it must hold:

1. $\mathbf{S} : \mathbf{V_A} \longrightarrow \mathbf{V_B}$ is an isomorphism of vector spaces, that is $\mathbf{S}$ is invertible, and
2. $\mathbf{S}(\mathbf{x} \cdot v) = \mathbf{x} \cdot (\mathbf{S}(v))$, that is $\mathbf{S}(\mathbf{A}(v)) = \mathbf{B}(\mathbf{S}(v))$, that is

$$\mathbf{SA} = \mathbf{BS}, \quad \text{or} \quad \mathbf{A} = \mathbf{S}^{-1}\mathbf{BS}$$

For the converse, read the equations backwards.

We will use this setup to solve

1. Given **A** and **B** as above, decide whether $\mathbf{A} \sim \mathbf{B}$.
2. Describe the vector space

$$\{\mathbf{B} \in \mathbf{M}_n(k) : \mathbf{AB} = \mathbf{BA}\}$$

3. Many other questions are answered.

Modules over PIDs

Let R be a PID and M a finitely generated R-module, $M = (u_1, \ldots, u_n)$, i.e. every $u \in M$ can be written

$$u = r_1 u_1 + \cdots + r_n u_n, \quad r_i \in R.$$

Examples are free R-modules, $M = R^n$, or

$$M = R/(d_1) \oplus \cdots \oplus R/(d_n).$$

Free Presentation

Definition

A free presentation of M is a surjective R-module homomorphism

$$\varphi : R^n = Re_1 \oplus \cdots \oplus Re_n \to M, \quad \varphi(e_i) = u_i.$$

The kernel of φ is the submodule

$$L = \{(a_1, \ldots, a_n) \in R^n : \sum a_i u_i = 0\}.$$

L is finitely generated (being a submodule of the Noetherian module R^n), and $R^n/L \simeq M$.

L is called the module of relations of the a_i, or a module of syzygies of M.

L has a set of generators

$$\begin{aligned} v_1 &= (a_{11}, \ldots, a_{1n}) \\ &\vdots \\ v_m &= (a_{m1}, \ldots, a_{mn}) \end{aligned}$$

which can be conveniently coded by the matrix

$$\mathbf{A} = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}$$

A is associated to the basis $\{e_1, \ldots, e_n\}$ of R^n and the generators $\{v_1, \ldots, v_m\}$ of L. We are going to change the two sets to make the quotient module R^n/M nice.
Consider elementary row operations on **A**, with the exception of dividing a row or column by a non-unit of R.

- For example, adding c times the first row to the second, has the effect of replacing the generator $v_2 \to v_2 + cv_1$, which does not change L. Similar effects for the other row operators.
- The interpretations of the column operations is the usual. For example, adding d times column 1, c_1, to column $c_2 \to c_2 + dc_1$, gives the representations of the vectors v_i in terms of the basis $\{e'_1 = e_1 - de_2, e_2, e_3, \ldots, e_n\}$.

Key Observation

Proposition

Let R be an Euclidean domain. Given a matrix $\mathbf{A}$ with entries in R, there exists a sequence of elementary row and column operations such that

$$\mathbf{A} \rightsquigarrow \begin{bmatrix} d_1 & 0 & 0 & \cdots & 0 \\ 0 & d_2 & 0 & \cdots & 0 \\ 0 & 0 & d_3 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \end{bmatrix}$$

where $d_1 | d_2 | d_3 | \cdots$. Furthermore, the ideals (d_i) are unique.

Remark

The same assertion holds for general PID's with one extra operation allowed (details soon).

Example

$$\begin{bmatrix} 2 & 4 & 6 \\ 5 & 3 & 0 \end{bmatrix} \longrightarrow \begin{bmatrix} 2 & 0 & 0 \\ 5 & -7 & -15 \end{bmatrix} \longrightarrow \begin{bmatrix} 2 & 0 & 0 \\ 1 & -7 & -15 \end{bmatrix}$$

$$\begin{bmatrix} 1 & -7 & -15 \\ 0 & 14 & 30 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 14 & 30 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix}$$

Proof

1. We induct on the size of the matrix $\mathbf{A}$.
2. The proof of termination comes from the fact that the division algorithm of R can place the gcd d_1 of all the entries of $\mathbf{A}$ in the position $(1, 1)$.
3. Now row and column operations are performed so that combined with those in step (1) give

$$\mathbf{A} \rightsquigarrow \mathbf{A}' = \begin{bmatrix} d_1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & \mathbf{B} & \\ 0 & & & \end{bmatrix}$$

4. This also shows that $d_1 | d_2 | d_3 | \cdots$.

Uniqueness

The uniqueness of the (d_i) comes from an additional observation.

1. The uniqueness of (d_1) comes directly from the construction.
2. To prove that of (d_2), we prove that $(d_1 d_2)$ is unique. This follows from the fact that just as every elementary operation leaves unchanged the gcd of the entries of the matrix, it also leaves unchanged the gcd of all 2×2 minors of $\mathbf{A}$ (or, more generally, of all $r \times r$ minors).

Structure Theorem for Modules over PID

Given a module $M = R^n/L$, there is a basis $e_1, e_2, \ldots, e_n$ of R^n, and a set of generators of L,

$$d_1 e_1, d_2 e_2, \ldots, d_n e_n.$$

This implies

$$M \simeq (Re_1/d_1 Re_1) \oplus \cdots \oplus (Re_n/d_n Re_n) \simeq R/(d_1) \oplus \cdots \oplus R/(d_n).$$

Some of the $d_i = 1$, and $R/(d_i) = 0$, or $d_i = 0$, and $R/(d_i) \simeq R$.

Theorem

Every finitely generated module M over a PID R is isomorphic to

$$R/(d_1) \oplus \cdots \oplus R/(d_n),$$

where $d_1 | d_2 | d_3 | \cdots$. The ideals (d_i) are uniquely determined, in particular the number r of $d_i = 0$, is uniquely determined (called torsionfree rank of M),

$$M \simeq R^r \oplus T,$$

where T has a nonzero annihilator. The ideals (d_i) are called the rational invariants of M.

There is just one point to add: For a PID, the $\gcd(a, b)$ is the generator of the ideal (a, b), that is

$$d = ra + sb, \quad (r, s) = (1).$$

This means that there exists α, β such that $r\alpha + s\beta = 1$.
Thus, if we have a matrix of relations **A**: if we have two rows v_1, v_2, an equivalent set of relations with v_1', v_2' replacing v_1, v_2 is

$$\begin{aligned} v_1' &= rv_1 + sv_2 \\ v_2' &= \alpha v_1 - \beta v_2 \end{aligned}$$

The first coordinate of v_1' is the gcd of the first coordinates of v_1 and v_2.
Such operations on columns give rise to basis changes in R^n.

The return of $\mathbf{V}_\varphi$

Let us go back to a linear transformation

$$\varphi : \mathbf{V} = k^n \longrightarrow k^n$$

and determine the structure of $\mathbf{V}_\varphi$.

Pick a k-basis $u_1, \ldots, u_n$ for $\mathbf{V}$, so that $\varphi = [c_{ij}]$. Let us determine a free presentation for $\mathbf{V}_\varphi$

$$0 \longrightarrow L \longrightarrow Re_1 \oplus \cdots \oplus Re_n \longrightarrow \mathbf{V}_\varphi \to 0, \quad e_i \to u_i.$$

The Syzygies of V_φ

Let us determine the module L. If

$$v = (\mathbf{f}_1(\mathbf{x}), \ldots, \mathbf{f}_n(\mathbf{x})),$$

$$\sum_{i=1}^{n} \mathbf{f}_i(\varphi)(u_i) = 0.$$

For instance, from

$$\varphi(u_i) = \mathbf{x}u_i = \sum c_{ij}u_j,$$

we have that the rows of the matrix lie in L

$$[c_{ij}] - \mathbf{x}\mathbf{I} = \begin{bmatrix} c_{11} - \mathbf{x} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} - \mathbf{x} & \cdots & c_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} - \mathbf{x} \end{bmatrix}$$

Proposition

L is generated by the rows of $\varphi - \mathbf{x}\mathbf{I}$.

Proof. Let $v = (\mathbf{f}_1(\mathbf{x}), \ldots, \mathbf{f}_n(\mathbf{x})) \in L$. We argue that v is a linear combination (with coefficients in R) of the rows of $\varphi - \mathbf{x}\mathbf{I}$.

- If all the $\mathbf{f}_i(\mathbf{x})$ constants, $\sum_i \mathbf{f}_i u_i = 0$ means that $\mathbf{f}_i = 0$, since the u_i are k-linearly independent.
- We induct on $\sup\{\deg(\mathbf{f}_i)\}$ and on the number of components of this degree. Say $\deg(\mathbf{f}_1) = \sup\{\deg(\mathbf{f}_i)\}$. Divide $\mathbf{f}_1$ by $c_{11} - \mathbf{x}$, $\mathbf{f}_1 = \mathbf{q}(c_{11} - \mathbf{x}) + r$,

$$(\mathbf{f}_1, \ldots, \mathbf{f}_n) - \mathbf{q}(c_{11} - \mathbf{x}, \ldots, c_{1n}) = (\mathbf{g}_1, \ldots, \mathbf{g}_n) = u.$$

  Note that u has fewer terms, if any, of degree $\geq \deg(\mathbf{f}_1)$.

Structure of $\mathbf{V}_\varphi$

It comes out of the algorithm

$$\varphi - \mathbf{x}\mathbf{I} \longrightarrow \begin{bmatrix} d_1(\mathbf{x}) & & & \\ & d_2(\mathbf{x}) & & \\ & & \ddots & \\ & & & d_n(\mathbf{x}) \end{bmatrix}$$

Corollary

If $d_i(\mathbf{x})$, $1 \le i \le n$, are the rational invariants of $\mathbf{V}_\varphi$

1. $\det(\varphi - \mathbf{x}\mathbf{I}) = (\text{unit}) d_1(\mathbf{x}) \cdots d_n(\mathbf{x})$.
2. **[Cayley-Hamilton Theorem]** .
3. $d_n(\mathbf{x})$ *is the minimal polynomial of* φ.

Example

$$\mathbf{V} = k^2, \quad 1/2 \in k, \quad \varphi = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$$

$$\begin{bmatrix} 1-x & 2 \\ 3 & 4-x \end{bmatrix} \to \begin{bmatrix} (1-x)/2 & 1 \\ 3 & 4-x \end{bmatrix} \to \begin{bmatrix} 1 & (1-x)/2 \\ 4-x & 3 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 \\ 0 & 3-(4-x)(1-x)/2 \end{bmatrix} \to \begin{bmatrix} 1 & 0 \\ 0 & x^2-5x-2 \end{bmatrix}$$

$$\mathbf{V}_\varphi = k[\mathbf{x}]/(\mathbf{x}^2 - 5\mathbf{x} - 2).$$

Scholium

Every square matrix **A** *with entries in a field is similar to its transpose.*

Proof. The rational invariants of $\mathbf{V_A}$ are determined from the gcd's of the minors of $\mathbf{A} - \mathbf{xI}$. But these are the same as the minors of

$$\mathbf{A}^t - \mathbf{xI} = (\mathbf{A} - \mathbf{xI})^t.$$

Commuting Matrices

Let φ be a linear trasformation of $\mathbf{V} = k^n$. Consider the set of linear transformations of $\mathbf{V}$ that commute with φ,

$$\mathbf{C}(\varphi) = \{\phi \in \mathbf{M}_n(k) : \phi\varphi = \varphi\phi\}.$$

We already interpreted such ϕ as a $k[\mathbf{x}]$-module homomorphism of $\mathbf{V}_\varphi$, that is, as an element of

$$\mathbf{C}(\varphi) = \mathrm{Hom}_{k[\mathbf{x}]}(\mathbf{V}_\varphi, \mathbf{V}_\varphi).$$

We use the structure of $\mathbf{V}_\varphi$ to determine this module.

Lemma

If $M = M_1 \oplus M_2 \oplus \cdots \oplus M_n$, *then*

$$\mathrm{Hom}_R(M, M) = \bigoplus_{1 \le i,j \le n} \mathrm{Hom}_R(M_i, M_j).$$

Theorem

For $r = k[\mathbf{x}]$, *if* $M = \mathbf{V}_\varphi = R/(d_1(\mathbf{x})) \oplus \cdots \oplus R/(d_n(\mathbf{x}))$, *then*

$$\mathbf{C}(\varphi) = \bigoplus_{1 \le i,j \le n} \mathrm{Hom}_R(R/(d_i(\mathbf{x})), R/(d_j(\mathbf{x}))).$$

The terms $\mathrm{Hom}_R(R/(d_i(\mathbf{x})), R/(d_j(\mathbf{x})))$ are easy to determine since one of the $d(\mathbf{x})$ divides the other.

Let us consider some special cases.

- Suppose the minimal polynomial of φ is equal to its characteristic polynomial. Such matrices are called derogatory. This means that $d_1 = \cdots = d_{n-1} = 1$, and $\mathbf{V}_\varphi = k[\mathbf{x}]/(d_n(\mathbf{x}))$. It follows that
$$\mathbf{C}(\varphi) = k[\mathbf{x}]/(d_n(\mathbf{x})),$$
which says that every endomorphism is a polynomial in φ, $\phi = \mathbf{g}(\varphi)$.
- Suppose that there are two summands, $M = R/(d_{n-1}) \oplus R/(d_n)$. We have $d_{n-1}|d_{n-1}$ to make calculation easy. The summands in $\mathrm{Hom}_R(M, M)$ are
$$\begin{aligned}
\mathrm{Hom}_R(R/(d_{n-1}), R/(d_{n-1})) &= R/(d_{n-1}) \\
\mathrm{Hom}_R(R/(d_n), R/(d_n)) &= R/(d_n) \\
\mathrm{Hom}_R(R/(d_{n-1}), R/(d_n)) &= R/(d_{n-1}) \\
\mathrm{Hom}_R(R/(d_n), R/(d_{n-1})) &= R/(d_{n-1})
\end{aligned}$$

Refinements

There are ways to enhance these decompositions that are useful, leading to primary decompositions in the case of modules over PID, or in the case of $\mathbf{V}_\varphi$ to Jordan decompositions.

They start out by applying the CRT (Chinese Remainder Theorem) (one in a class of results called partition of the unity) to the ring $R/(d)$, where R is a PID and d has a primary decomposition

$$d = p_1^{e_1} \cdots p_n^{e_n}.$$

Historical Example

Consider $360 = 2^3 \cdot 3^2 \cdot 5$.

$$\gcd(72, 45, 40) = 1, \quad \text{thus}$$

$$\exists a, b, c \in \mathbb{Z}, \quad 1 = 72a + 45b + 40c$$

that is, we can find the fraction $1/360$ as the combination

$$\frac{1}{360} = a\frac{1}{5} + b\frac{1}{8} + c\frac{1}{9}$$

Primary Decomposition

Proposition

If R is a PID and

$$d = p_1^{e_1} \cdots p_n^{e_n},$$

then

$$R/(d) = R/(p_1^{e_1}) \oplus \cdots \oplus R/(p_n^{e_n}).$$

Proof. Consider the elements $c_i = d/p_i^{e_i}$. Since $\gcd(c_1, \ldots, c_n) = 1$, there are elements $a_i \in R$ such that

$$1 = \sum_{i=1}^{n} a_i c_i.$$

Now define the homomorphism of R (check this is well defined!)

$$\mathbf{h} : R/(d) \longrightarrow R/(p_1^{e_1}) \oplus \cdots \oplus R/(p_n^{e_n}),$$

for $u \in R/(d)$

$$\mathbf{h}(u) = (a_1 u, \ldots, a_n u).$$

Exercise: Prove that h is one-one & onto.

Uniqueness–I

Theorem

Let R is a PID and A a finitely generated torsion module. If

$$A = \mathbf{W}_1 \oplus \cdots \oplus \mathbf{W}_m$$

is a primary decomposition the $\mathbf{W}_i$ are uniquely determined by A.

Proof. If $\mathbf{W}$ is one of the $\mathbf{W}_i$ then $\mathbf{W}$ is a direct sum of submodules isomorphic to $R/(p^r)$ for a unique prime p. This shows that $\mathbf{W}$ is annihilated by some p^s (s the largest of the exponents r:

$$\mathbf{W} = \{x \in A : p^r x = 0, \quad \text{some } r\}$$

Uniqueness–II

Theorem

Let R be a PID and $\mathbf{W}$ a finitely generated primary R-module. Given a decomposition

$$\mathbf{W} \simeq R/(p^{e_1}) \oplus \cdots \oplus R/(p^{e_m}),$$

where the exponents as listed as $e_1 \geq e_2 \geq \cdots \geq e_m$, the sequence $(e_1, e_2, \ldots, e_m)$ is uniquely determined by $\mathbf{W}$.

Proof. Consists of the following observations:

- $p\mathbf{W}$ is a submodule of $\mathbf{W}$ and $\mathbf{W}/p\mathbf{W}$ is isomorphic to

$$\mathbf{W}/p\mathbf{W} \simeq \oplus R/(p^{e_i})/pR/(p^{e_i})$$

- Each module $R/(p^e)/pR/(p^e))$ is isomorphic to $R/(p)$. Thus $\mathbf{W}/p\mathbf{W}$ is a vector space of dimension m over $R/(p)$.

- e_m is the smallest exponent such that $p^{e_m}\mathbf{W} = 0$
- Note $pR/(p^e) \simeq R/(p^{e-1})$
- Consider the module $p\mathbf{W}$. Its primary decomposition is

$$p\mathbf{W} \simeq R/(p^{e_1-1}) \oplus \cdots \oplus R/(p^{e_m-1})$$

Primary decomposition of $\mathbf{V}_\varphi$

In the cyclic decomposition

$$\mathbf{V}_\varphi = R/(d_1) \oplus \cdots \oplus R/(d_n)$$

we are going to replace each $R/(d_i)$ by its primary decomposition. Suppose $p_1, \ldots, p_m$ are the primes that occur. This leads to the primary decomposition of $\mathbf{V}_\varphi$

$$\mathbf{V}_\varphi = \mathbf{W}_1 \oplus \cdots \oplus \mathbf{W}_m$$

where $\mathbf{W}_i$ is a direct sum of modules $R/(p_i^{a_{ij}})$ for the same p_i.

Setting up matrix representation

Since φ acts as a homomorphism on $\mathbf{V}_\varphi$, and the $\mathbf{W}_i$ are submodules

$$\varphi : \mathbf{W}_i \to \mathbf{W}_i$$

this has the following consequence:

Block Decomposition

The decomposition of $\mathbf{V}_\varphi$ into a direct sum of modules $\mathbf{W}_1 \oplus \cdots \oplus \mathbf{W}_m$ leads to a block decomposition for any matrix representation of φ:

$$[\varphi] = \begin{bmatrix} [\varphi]_1 & \cdots & O \\ \vdots & \ddots & \vdots \\ O & \cdots & [\varphi]_m \end{bmatrix}$$

We are going to pick appropriate k-vector spaces in the submodules.

Jordan Block

Suppose the submodule $\mathbf{W}$ of $\mathbf{V}_\varphi$ is $k[\mathbf{x}]/(x-\lambda)^r$. This means that λ is an eigenvalue of φ. Let us look at one such $r \times r$ block

$$[\varphi]_{\mathbf{W}} = \mathbf{A} = [v_1|\cdots|v_r] = \begin{bmatrix} \lambda & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda & 1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda \end{bmatrix}$$

$$\underbrace{\mathbf{A}(u_1) = \lambda u_1}_{\text{eigenvector}}, \quad \mathbf{A}(u_2) = u_1 + \lambda u_2, \cdots, \mathbf{A}(u_r) = u_{r-1} + \lambda u_r$$

Jordan Basis

The k-vector space $k[\mathbf{x}]/(\mathbf{x}-\lambda)^r$ has many interesting bases, for instance the residue classes of $\{1, \mathbf{x}, \ldots, \mathbf{x}^{r-1}\}$.

Jordan's claim to glory comes from picking

$$\{v_1 = 1, v_2 = (\mathbf{x}-\lambda), \ldots, v_r = (\mathbf{x}-\lambda)^{r-1}\}$$

$$\begin{aligned}
\mathbf{x}(v_i) &= \mathbf{x}(\mathbf{x}-\lambda)^{i-1}, \quad i < r-1 \\
&= (\mathbf{x}-\lambda)^i + \lambda(\mathbf{x}-\lambda)^{i-1} \\
&= \lambda v_i + v_{i+1} \\
\mathbf{x}(v_r) &= \lambda v_r
\end{aligned}$$

Now reverse the notation: $u_i = v_{r+1-i}$.

We collect all the blocks (from the $\mathbf{W}_i$) for the same eigenvalue

$$\begin{bmatrix} \boxed{\mathbf{J}_1} & O & O \\ O & \boxed{\mathbf{J}_2} & O \\ O & O & \boxed{\mathbf{J}_3} \end{bmatrix} = \begin{bmatrix} \lambda & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \lambda & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \lambda & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \lambda & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \lambda & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda \end{bmatrix}$$

Jordan Decomposition Theorem

Theorem

Any linear operator $\mathbf{T}$ *whose characteristic polynomial* $p(x) = \pm \prod_{i=1}^{m} (x - \lambda_i)^{n_i}$ *splits has a unique matrix representation into blocks*

$$[\mathbf{T}]_{\mathcal{B}} = \begin{bmatrix} \mathbf{A}_1 & \cdots & O \\ \vdots & \ddots & \vdots \\ O & \cdots & \mathbf{A}_m \end{bmatrix}$$

where each $\mathbf{A}_i$ *has a representation by Jordan* λ_i*-blocks whose number and sizes are uniquely defined*

$$\begin{bmatrix} \lambda_i & 1 & \cdots & 0 \\ 0 & \lambda_i & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_i \end{bmatrix}.$$

Outline

Assignment #11

Do any 2 problems:

- For the rational tridiagonal matrix [if too laborious, do 6×6]

$$\varphi = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

  find: (a) its rational invariants, including its minimal polynomial; (b) the dimension of the subspace of 8×8 matrices commuting with it.

- Let φ and ψ be $n \times n$ matrices with entries in a field **K.** If there is an invertible matrix S over an extension field **F** such that

$$\psi = S \cdot \varphi \cdot S^{-1},$$

  [that is, φ and ψ are similar over **F**] show that φ and ψ are similar over **K.**
- Describe a Jordan's canonical form theorem over the real numbers. [Only looks vague!]
- If the integer n has a prime factorization

$$n = p_1^{r_1} \cdots p_m^{r_m},$$

  find a 'formula' for the number of isoclasses of abelian groups of order n.

Infinitely generated modules

Let us begin with $\mathbb{Q}$ viewed as a $\mathbb{Z}$-module.

- First we find a convenient set of generators of $\mathbb{Q}$: For $n \in \mathbb{N}$, consider the subgroup of $\mathbb{Q}$ given by $\mathbb{Z}\frac{1}{n!}$. Then

$$\mathbb{Q} = \bigcup_{\rightarrow} \mathbb{Z}\frac{1}{n!}$$

- Now let F be a free abelian group with a basis $\{e_n\}$. Map this element to $\frac{1}{n!}$. Let L be the subgroup of F generated by the syzygies $ne_n - e_{n-1}, n \geq 2$.
- L is a free abelian group and $F/L \simeq \mathbb{Q}$.

Theorem

Let R be a PID. Then any submodule of a free module is free.

Proof. Let F be a free module with basis $\{e_i, i \in I\}$, and suppose the index set I is well-ordered. For each $i \in I$ set

$$F_i = \bigoplus_{j<i} Re_j,$$

with $F_0 = 0$ and $F_{i+1} = \bigoplus_{j \leq i} Re_j$.
For a submodule M of F each $x \in M \cap F_{i+1}$ has a unique expression $x = y + re_i$, where $y \in F_i$ and $r \in R$. If $\phi_i : M \cap F_{i+1} \to R$ is defined by $\phi_i(x) = r$, there is a SES

$$0 \to M \cap F_i \longrightarrow M \cap F_{i+1} \longrightarrow I_i \to 0,$$

where $I_i = \mathrm{image}\ \phi_i$. Since I_i is projective, the sequence splits: $M \cap F_{i+1} = (M \cap F_i) \oplus C_i$, $C_i \simeq I_i$. We claim $M = \bigoplus_i C_i$.

Proof cont'd

Claim: $M = (\bigcup C_i)$: Since $F = \bigcup F_i$, each $x \in M$ lies in some F_{i+1}. Let $\nu(x)$ be the smallest i such that $x \in F_{i+1}$.
Clearly $C = (\bigcup C_i) \subset M$. If $C \neq M$, consider the set

$$\{\nu(x) : x \in M, x \notin C\} \subset I$$

Let j be the least such index and choose $y \in M$ with $y \in M \setminus C$ and $\nu(y) = j$. This last implies $y \in M \cap F_{j+1}$, so $y = b + c$, $b \in M \cap F_j$ and $c \in C_j$. Therefore $b = y - c \in M$, $b \notin C$ (unless $y \in C$), and $\nu(b) < j$, a contradiction. Hence $M = C$.

Proof concl'd

To prove $M = \bigoplus C_i$, suppose $c_1 + \cdots + c_n = 0$, $c_i \in C_{k_i}$, $k_1 < \cdots < k_n$. Then

$$c_1 + \cdots + c_{n-1} = c_n \in (M \cap F_{k_n}) \cap C_{k_n} = 0$$

It follows that $c_n = 0$. Induction gives c_i for all i.

Outline

Class discussion

Let $\mathbf{f}(\mathbf{x}) = \mathbf{f}(x_1, \ldots, x_n)$ be a nonconstant polynomial of $R = \mathbb{C}[\mathbf{x}] = \mathbb{C}[x_1, \ldots, x_n]$, $n > 1$.

Fact: There is $\mathbf{c} \in \mathbb{C}^n$ such that $\mathbf{f}(\mathbf{c}) = 0$.
Task: Volunteer to the plate!

The answer is easy when

$$\mathbf{f}(x_1, \ldots, x_n) = x_n^d + \mathbf{g}(x_1, \ldots, x_n),$$

where $\mathbf{g}(\mathbf{x})$ is a polynomial of degree $< d$ in the variable x_n. So what is the solution for the general case? One seeks a change of variables (possibly linear)

$$\begin{aligned} \mathbf{x} &\rightarrow \mathbf{y}, \quad [\mathbf{x}] = [\mathbf{y}]\mathbf{A} \\ \mathbf{f}(\mathbf{x}) &= \mathbf{f}(\mathbf{yA}) = \mathbf{g}(\mathbf{y}) \end{aligned}$$

so that $\mathbf{g}(\mathbf{y})$ has the appropriate form.

More generally, let $\mathbf{f}_1(\mathbf{x}), \ldots, \mathbf{f}(\mathbf{x}_m)$ be a set of elements of $R = \mathbb{C}[\mathbf{x}]$.

Question: What are the obstructions to finding $\mathbf{c} \in \mathbb{C}^n$ such that

$$\mathbf{f}_1(\mathbf{c}) = \mathbf{f}_2(\mathbf{c}) = \cdots = \mathbf{f}_m(\mathbf{c}) = 0\ ?$$

Obviously one is: there exist $\mathbf{g}_1(\mathbf{x}), \ldots, \mathbf{g}_m(\mathbf{x})$ such that

$$\mathbf{g}_1(\mathbf{x})\mathbf{f}_1(\mathbf{x}) + \cdots + \mathbf{g}_m(\mathbf{x})\mathbf{f}_m(\mathbf{x}) = 1$$

What else?

Hilbert Nullstellensatz

Let k be a field and denote by $\overline{k}$ its algebraic closure. The Hilbert Nullstellensatz is about qualitative results about systems of polynomial equations.

Let $\mathbf{f}_i(x_1, \ldots, x_n) \in R = k[x_1, \ldots, x_n]$, $1 \leq i \leq m$, be a set of polynomials.

Definition

The algebraic variety defined by the $\mathbf{f}_i$ is the set

$$V(\mathbf{f}_1, \ldots, \mathbf{f}_m) = \{\mathbf{c} = (c_1, \ldots, c_n) \in \overline{k}^n : \mathbf{f}_i(\mathbf{c}) = 0, \quad 1 \leq i \leq m.\}$$

A hypersurface is a variety defined by a single equation $V(\mathbf{f})$.

Remark

If I is the ideal generated by the $\mathbf{f}_i$, then $V(I) = V(\mathbf{f}_1, \ldots, \mathbf{f}_m)$.

Hilbert Nullstellensatz

Theorem

If the ideal $I \subset R = k[x_1, \ldots, x_n]$ is proper, i.e. $I \neq R$, then $V(I) \neq \emptyset$.

Proof. We make two reductions.

1. Let $\mathfrak{m}$ be a maximal ideal of R containing I. Since $V(\mathfrak{m}) \subset V(I)$, ETA that I is maximal.
2. The ring of polynomials $S = \overline{k}[x_1, \ldots, x_n]$ is integral over $R = k[x_1, \ldots, x_n]$. By Lying-over, there is a maximal ideal M of S such that $M \cap R = \mathfrak{m}$. Since $V(M) \subset V(\mathfrak{m})$, ETA that I is a maximal ideal and k is algebraically closed.

Nullstellensatz

After these reductions the assertion is:

Theorem

If k is an algebraically closed field and M is a maximal ideal of $R = k[x_1, \ldots, x_n]$, then there is

$$\mathbf{c} = (c_1, \ldots, c_n) \in k^n$$

such that

$$\mathbf{f}(\mathbf{c}) = 0 \quad \forall \mathbf{f}(\mathbf{x}) \in M.$$

Special case: $\mathbb{C}$

Consider the field $\mathbf{F} = \mathbb{C}[x_1, \ldots, x_n]/M$.

Proposition

It is ETS that $\mathbf{F}$ *is isomorphic to* $\mathbb{C}$*.*

Proof. Indeed, if $\mathbf{F} \simeq \mathbb{C}$, for each indeterminate x_i its equivalence class in $k[x_1, \ldots, x_n]/M$ contains some element c_i of $\mathbb{C}$, that is $x_i - c_i \in M$. this means that

$$(x_1 - c_1, \ldots, x_n - c_n) \subset M.$$

But $(x_1 - c_1, \ldots, x_n - c_n)$ is also a maximal ideal, therefore it is equal to M. Clearly every polynomial of M vanishes at $\mathbf{c} = (c_1, \ldots, c_n)$. □

Proof of $\mathbb{C} = \mathbb{C}[x_1, \ldots, x_n]/M$

1. ETS that the extension $\mathbb{C} \to \mathbf{F} = \mathbb{C}[x_1, \ldots, x_n]/M$ is algebraic.
2. Observe that $[\mathbf{F} : \mathbb{C}]$ is countable, $\mathbf{F}$ being a homomorphic image of the countably generated vector space $\mathbb{C}[x_1, \ldots, x_n]$.
3. If $\mathbf{F}$ is not algebraic over $\mathbb{C}$, suppose $t \in \mathbf{F}$ is transcendental over $\mathbb{C}$.
4. Consider the uncountable set $\{1/(t - c), c \in \mathbb{C}\}$.

Since they cannot be linearly independent, there are distinct c_i, $1 \leq i \leq m$ and nonzero $r_i \in \mathbb{C}$ such that

$$r_1 \frac{1}{t - c_1} + \cdots + r_m \frac{1}{t - c_m} = 0.$$

Clearing denominators gives the equality of two polynomials of $\mathbb{C}[t]$:

$$r_1(t - c_2)(t - c_3)\cdots(t - c_m) = (t - c_1)\mathbf{g}(t),$$

which is a contradiction as the c_i are distinct.

Outline

NNL: Noether Normalization Lemma

Definition

A finitely generated algebra R over a field k is a homomorphic image of a ring of polynomials over k,

$$k[x_1, \ldots, x_n]/I \simeq R = k[a_1, \ldots, a_n].$$

Theorem (NNL)

If R is finitely generated over k, there is a subalgebra

$$S = k[y_1, \ldots, y_r] \hookrightarrow R$$

such that the y_i are algebraically independent and R is integral over S. S is called a Noether Normalization of R.

From NN to Nullstellensatz

1. Let M be a maximal ideal of $k[x_1, \ldots, x_n]$, $k = \overline{k}$. We will show that $M = (x_1 - c_1, \ldots, x_n - c_n)$, $c_i \in k$.
2. Using the NNL, let $S = k[y_1, \ldots, y_r] \hookrightarrow R = k[x_1, \ldots, x_n]/M$ be a Noether normalization. Since R is a field, S is also a field, thus $r = 0$.
3. This gives that $S = k \to R$ is a finite extension, so $k = R$.

Another version of the Nullstellensatz

Theorem

Let I be an ideal of $R = k[x_1, \ldots, x_n]$ and $\mathbf{f} \in R$ a polynomial. Then

$$V(I) \subset V(\mathbf{f}) \Leftrightarrow \mathbf{f} \in \sqrt{I}$$

that is, there is a power $\mathbf{f}^r \in I$.

Proof. In one direction it is clear.

Suppose $V(I) \subset V(\mathbf{f})$. Consider the ideal L in the polynomial ring with one extra variable

$$L = (I, 1 - t\mathbf{f}) \subset k[x_1, \ldots, x_n, t].$$

Since each zero of I is a zero of $\mathbf{f}$, $L = (I, 1 - t\mathbf{f})$ has no zeros. Thus by the Nullstellensatz $L = (1)$. This means that there is an equation

$$\sum \mathbf{g}_i \mathbf{f}_i + (1 - t\mathbf{f})\mathbf{g} = 1, \quad \mathbf{f}_i \in I, \mathbf{g}_i, \mathbf{g} \in R[t].$$

Replacing $t \to 1/\mathbf{f}$ and clearing denominators gives an equation

$$\mathbf{f}^r = \sum \mathbf{h}_i \mathbf{f}_i, \quad \mathbf{h}_i \in R$$

Example

Let

$$R = k[x, y]/(y^2 - 2xy + x^3)$$

Set $y_1 = \overline{x}$ and

$$S = k[y_1] \subset R$$

Note that $\overline{y}$ is integral over S, so R is integral over S. Finally,

$$S \simeq k[x]/(k[x] \cap (y^2 - 2xy + x^3)) = k[x]$$

Example

1. If $R = k[x, y]/(xy + x + y)$, need a preparation: change variables $x \to x_1$, $y \to x_1 + y_1$, so

$$xy + x + y \to x_1(x_1 + y_1) + x_1 + x_1 + y_1 = x_1^2 + x_1 y_1 + 2x_1 + y_1$$

2. Get the NN by choosing

$$S = k[y_1] \hookrightarrow R = k[x, y]/(xy + x + y).$$

Proof of NN

Let R be a commutative ring and B a finitely generated R-algebra, $B = R[x_1, \ldots, x_d]$. The expression *Noether normalization* usually refers to the search-as effectively as possible-of more amenable finitely generated R-subalgebras $A \subset B$ over which B is finite. This allows for looking at B as a finitely generated A-module and therefore applying to it methods from homological algebra or even from linear algebra.

When R is a field, two such results are: (i) the classical *Noether normalization lemma*, that asserts when it is possible to choose A to be a ring of polynomials, or (ii) how to choose A to be a hypersurface ring over which B is birational. We review these results since their constructive steps are very useful in our discussion of the integral closure of affine rings.

Affine Rings

Let $B = k[x_1, \ldots, x_n]$ be a finitely generated algebra over a field k and assume that the x_i are algebraically dependent. Our goal is to find a new set of generators $y_1, \ldots, y_n$ for B such that

$$k[y_2, \ldots, y_n] \hookrightarrow B = k[y_1, \ldots, y_n]$$

is an integral extension.

Let $k[X_1, \ldots, X_n]$ be the ring of polynomials over k in n variables; to say that the x_i are algebraically dependent means that the map

$$\pi\colon\ k[X_1, \ldots, X_n] \to B, \quad X_i \mapsto x_i$$

has non-trivial kernel, call it I.

Assume that f is a nonzero polynomial in I,

$$f(X_1, \ldots, X_n) = \sum_{\alpha} a_\alpha X_1^{\alpha_1} X_2^{\alpha_2} \cdots X_n^{\alpha_n},$$

where $0 \neq a_\alpha \in k$ and all the multi-indices $\alpha = (\alpha_1, \ldots, \alpha_n)$ are distinct. Our goal will be fulfilled if we can change the X_i into a new set of variables, the Y_i, such that f can be written as a monic (up to a scalar multiple) polynomial in Y_1 and with coefficients in the remaining variables, i.e.

$$f = aY_1^m + b_{m-1} Y_1^{m-1} + \cdots + b_1 Y_1 + b_0, \tag{1}$$

where $0 \neq a \in k$ and $b_i \in k[Y_2, \ldots, Y_n]$.

We are going to consider two changes of variables that work for our purposes: the first one, a clever idea of Nagata, does not assume anything about k; the second one assumes k to be infinite and has certain efficiencies attached to it.

The first change of variables replaces the X_i by Y_i given by

$$Y_1 = X_1,\ \ Y_i = X_i - {X_1}^{p^{i-1}} \text{for } i \geq 2,$$

where p is some integer yet to be chosen.
If we rewrite f using the Y_i instead of the X_i, it becomes

$$f = \sum_{\alpha} a_\alpha Y_1^{\alpha_1}(Y_2 + Y_1^p)^{\alpha_2} \cdots (Y_n + Y_1^{p^{n-1}})^{\alpha_n}. \qquad (2)$$

Expanding each term of this sum, there will be only one term pure in Y_1, namely

$$a_\alpha Y_1^{\alpha_1+\alpha_2 p+\cdots+\alpha_n p^{n-1}}.$$

Furthermore, from each term in (2) we are going to get one and only one such power of Y_1. Such monomials have higher degree in Y_1 than any other monomial in which Y_1 occurs. If we choose $p > \sup\{\alpha_i \mid a_\alpha \neq 0\}$, then the exponents $\alpha_1 + \alpha_2 p + \cdots + \alpha_n p^{n-1}$ are distinct since they have different p-adic expansions. This provides for the required equation.

If k is an infinite field, we consider another change of variables that preserves degrees. It will have the form

$$Y_1 = X_1,\ Y_i = X_i - c_i X_1 \text{ for } i \geq 2,$$

where the c_i are to be properly chosen. Using this change of variables in the polynomial f, we obtain

$$f = \sum_{\alpha} a_\alpha Y_1^{\alpha_1} (Y_2 + c_2 Y_1)^{\alpha_2} \cdots (Y_n + c_n Y_1)^{\alpha_n}. \qquad (3)$$

We want to make choices of the c_i in such a way that when we expand (3) we achieve the same goal as before, i.e. a form like that in (1). For that, it is enough to work on the homogeneous component f_d of f of highest degree, in other words, we can deal with f_d alone. But

$$f_d(Y_1, \ldots, Y_n) = h_0(1, c_2, \ldots, c_n) Y_1^d + h_1 Y_1^{d-1} + \cdots + h_d,$$

where h_i are homogeneous polynomials in $k[Y_2, \ldots, Y_n]$, with $\deg h_i = i$, and we can view $h_0(1, c_2, \ldots, c_n)$ as a nontrivial polynomial function in the c_i. Since k is infinite, we can choose the c_i, so that $0 \neq h_0(1, c_2, \ldots, c_n) \in k$.

Theorem (Noether Normalization)

Let k be a field and $B = k[x_1, \ldots, x_n]$ a finitely generated k-algebra; then there exist algebraically independent elements $z_1, \ldots, z_d$ of B such that B is integral over the polynomial ring $A = k[z_1, \ldots, z_d]$.

Proof. We may assume that the x_i are algebraically dependent. From the preceding, we can find $y_1, \ldots, y_n$ in B such that

$$k[y_2, \ldots, y_n] \hookrightarrow k[y_1, \ldots, y_n] = B$$

is an integral extension, and if necessary we iterate. □

Corollary

Let k be a field and $\psi : A \mapsto B$ a k-homomorphism of finitely generated k-algebras. If $\mathfrak{P}$ is a maximal ideal of B then $\mathfrak{p} = \psi^{-1}(\mathfrak{P})$ is a maximal ideal of A.

Proof. Consider the embedding

$$A/\mathfrak{p} \hookrightarrow B/\mathfrak{P}$$

of k-algebras, where by the preceding $B/\mathfrak{P}$ is a finite dimensional k-algebra. It follows that the integral domain $A/\mathfrak{p}$ is also a finite dimensional k-vector space and therefore must be a field. $\square$

Outline

Assignment #12

Do Problem #2 only

1. Describe [with proofs] the prime spectrum of $k[x, y]$, k a field.
2. If M is a maximal ideal of $R = \mathbb{R}[x, y]$, prove that $\dim_{\mathbb{R}} R/M$ is 1 or 2.

Outline

Invertible Ideals

Let R be an integral domain of field of fractions $\mathbf{K}$. The ideals of R are part of an important class of R-submodules of $\mathbf{K}$:

Definition

A submodule L of $\mathbf{K}$ is fractionary if there is $0 \neq d \in R$ such that $dL \subset R$.

1. This means that $L = d^{-1}Q$, where Q is an ideal of R.
2. $\mathbf{K}$ is not fractionary, unless $R = \mathbf{K}$.

The sum and the product of fractionary ideals is fractionary. Another operation is

Definition

The quotient of two fractionary ideals is

$$L_1 : L_2 = \{x \in \mathbf{K} : xL_2 \subset L_1\}.$$

In particular

$$R : L = \{x \in \mathbf{K} : xL \subset R\}.$$

L_1 is said to be invertible if there is a fractionary ideal L_2 such that $L_1 \cdot L_2 = R$.

Invertible Ideals

Proposition

If L is an invertible ideal of R, then L is a finitely generated R-module.

Proof.

The equality $L \cdot L' = R$ means that there are $x_i \in L$, $y_i \in L'$, $1 \le i \le n$, such that

$$1 = x_1 y_1 + \cdots + x_n y_n.$$

Thus for any $x \in L$,

$$x = (xy_1)x_1 + \cdots + (xy_n)x_n$$

which shows that $L_1 = (x_1, \ldots, x_n)$ since all $xy_i \in R$. □

Example

Let $R = \mathbb{Z}[\sqrt{-5}]$, $I = (3, 2+\sqrt{-5})$. We claim that I is an invertible ideal. We will also see that I is not a principal ideal.

- $9 = 3 \cdot 3 = (2+\sqrt{-5})(2-\sqrt{-5})$
- Set $J = (1, \frac{3}{2+\sqrt{-5}})$
- $I \cdot J = (2+\sqrt{-5}, 3, 2-\sqrt{-5}) = (1) = R$

Local Rings

Proposition

If R is a local ring, then every invertible fractionary ideal is principal.

Proof.

Denote by $\mathfrak{m}$ the unique maximal ideal of R. If L is invertible, $L \cdot L' = R$, in the equation

$$1 = x_1 y_1 + \cdots + x_n y_n,$$

some product, say $x_1 y_1 \notin \mathfrak{m}$. This means that it is an invertible element of R. Thus, for any $x \in L$,

$$x = (x_1 y_1)^{-1} (y_1 x) x_1,$$

that is $L = Rx_1$. □

Outline

Dedekind Domains

These are important rings. The interest springs from their sources:

- Number Theory: Rings of algebraic numbers: If **L** is a finite extension of $\mathbb{Q}$, R is the ring of elements of **L** integral over $\mathbb{Z}$.
- Algebraic Geometry: (Case of plane curve) $R = k[x, y]/(\mathbf{f}(x, y))$, or its integral closure.

Dedekind Domains

The formal definition is:

Definition

The integral domain $\mathfrak{D}$ is a Dedekind domain if every ideal is invertible.

- $\mathfrak{D}$ is a nice notation for D.D.'s, but we shall use plain R...
- The inverse of a fractionary ideal L is denoted L^{-1} (it is unique).
- Of course every fractionary ideal will be invertible as well.
- If R is a Dedekind domain, it is Noetherian.
- Besides PID's, what are they like?

Properties of D.D.'s

Theorem

If R is a Dedekind domain then every nonzero prime ideal is maximal.

Proof.

We will argue by contradiction. Let $P \subsetneq Q$ be distinct prime ideals. We are going to form the ring of fractions $S = R_Q$ (Recall ...). S is a local ring and P_Q and Q_Q are distinct prime ideals. They are both invertible. Thus

$$P_Q = Sa \subsetneq Sb = Q_Q$$

with $a = cb$, and therefore $c \in P_Q$ since $b \notin P_Q$. Thus

$$c = ra = b^{-1}a,$$

Factorization

Theorem

Let R be a Dedekind domain. Then any nonzero ideal I has a unique factorization

$$I = P_1^{e_1} \cdots P_n^{e_n},$$

where the P_i are distinct prime idealas.

Proof. Since R is Noetherian, I has a primary decomposition

$$I = Q_1 \cap \cdots \cap Q_n,$$

where the $P_i = \sqrt{Q_i}$ are distinct maximal ideals.

We want to argue that the intersection is actually a product.

Definition

Two ideals J and L are co-maximal if $J + L = R$.

Lemma

If J and L are co-maximal ideals, then $JL = J \cap L$.

Proof.

It is clear that $JL \subset J \cap L$. For the converse, let $x \in J \cap L$. Since $J + L = R$, there are $a \in J$ and $b \in L$ such that

$$\begin{aligned} 1 &= a + b, \quad \text{hence} \\ x &= xa + xb, \quad \text{with} \quad xa, xb \in J \cap L \end{aligned}$$

□

Now we apply this to $I = Q_1 \cap L$, $L = Q_2 \cap \cdots \cap Q_n$. To see that Q_1 and L are co-maximal, deny. Then $Q_1 + L \subseteq M$ for some maximal ideal M. This ideal would contain $\sqrt{Q_1}$ and $Q_2 \cdots Q_n$. Thus M would contain two other maximal ideals, a contradiction.

Primary ideals

Proposition

Let R be a Dedekind domain. If Q is a P-primary ideal, then $Q = P^e$, for some $e \geq 1$.

Proof.

Since the radical of Q is P, some power of P is contained in Q, say $P^e \subseteq Q$, with e as small as possible. If the containement is proper, we have

$$P^e \cdot Q^{-1} \subsetneq Q \cdot Q^{-1} = R.$$

Therefore we must have

$$\begin{aligned} P^e \cdot Q^{-1} &\subseteq P \quad \text{and therefore} \\ P^{e-1} &\subseteq Q \quad \text{which is a contradiction.} \end{aligned}$$

Corollary

If R is a Dedekind domain, the nonzero fractionary ideals form a multiplicative group $\mathbf{G}$, with the nonzero principal fractionary forming a subgroup $\mathbf{P}$. The quotient $\mathbf{G}/\mathbf{P}$ is called the class group $\mathbf{C}(R)$ of R. R is a PID if and only if $\mathbf{C}(R)$ is trivial.

Remarks

1. Recall that if $R \subset S$ are rings, an element $u \in S$ is integral over R if it satisfies a monic equation with coefficients in R, $u^n + r_1 u^{n-1} + \cdots + r_n = 0$, $r_i \in R$.
2. If every element of S that is integral over R already lies in R, R is said to be **integrally closed** in S.
3. If R is a domain of field of fractions $\mathbf{K}$ and $\mathbf{L}$ is a finite extension of $\mathbf{K}$, for any $u \in \mathbf{L}$ there is an equation $u^n + r_1 u^{n-1} + \cdots + r_n = 0$, $r_i \in \mathbf{K}$. Let $0 \neq d \in R$ such that $dr_i \in R$ (d is a **common denominator** of the r_i.) Then $d^n u^n + dr_1 d^{n-1} u^{n-1} + \cdots + d^n r_n = 0$, $r_i \in \mathbf{K}$, showing that du is integral over R.

Characterization of D.D.'s

Theorem

Let R be an integral domain of field of fractions $\mathbf{K}$. The following are equivalent:

1. *R is a Dedekind domain.*
2. *R is a Noetherian ring in which every nonzero prime ideal is maximal and R is integrally closed in $\mathbf{K}$.*
3. *R is Noetherian and for each prime ideal P the localization R_P is a PID.*

We will check the equivalences:

$$(1) \Leftrightarrow (2) \Leftrightarrow (3)$$

Some remarks on localization

- If R is an integral domain then

$$R = \bigcap_P R_P, \quad \text{all maximal ideals } P$$

Indeed, if x is contained in each R_P,

$$x = a/b, \quad b \notin P,$$

the set (an ideal) of all elements d (denominators) such that $dx \in R$ is not contained in any maximal ideal of R, so must be R.

- If each R_P is integrally closed, then their intersection will also be such: If $z \in \mathbf{K}$ is integral over R, it is also integral over the larger R_P. Thus $z \in R_P$.

Characterization of a PID with a unique maximal ideal

Proposition

Let R be a Noetherian domain with a unique nonzero prime ideal $\mathfrak{m}$. R is a PID if and only if R is integrally closed.

Proof. ETS that if R is integrally closed then $\mathfrak{m}$ is invertible.

- Let $0 \neq x \in \mathfrak{m}$. Then the radical $\sqrt{(x)}$ of (x) is $\mathfrak{m}$.
- Let n be the smallest integer such that $\mathfrak{m}^n \subset (x)$. Consider the product

$$(1/x)\mathfrak{m}^{n-1}\mathfrak{m} \subset R$$

- If $(1/x)\mathfrak{m}^{n-1}\mathfrak{m} = R$, $\mathfrak{m}$ is invertible.

- If not, $(1/x)\mathfrak{m}^{n-1}\mathfrak{m} \subset \mathfrak{m}$.
- Recall the Cayley-Hamilton for modules: If E is a faithful, finitely generated R-module and z is an element of a larger ring such that $z \cdot M \subset M$, then z is integral over R.
- This implies that $(1/x)\mathfrak{m}^{n-1}$ is integral over R, therefore is contained in R, since it is integrally closed, that is $\mathfrak{m}^{n-1} \subset (x)$, which contradicts the choice of n.

Taylor expansion

It is useful to keep in mind the formula for the Taylor expansion of a polynomial $\mathbf{f}(x, y)$ around the point (a, b)
Use the notation

$$b_{mn} = \frac{\partial^{m+n}\mathbf{f}}{\partial^m x \partial^n y}(a, b)$$

$$\begin{aligned}\mathbf{f}(x, y) &= \mathbf{f}(a, b) + b_{10}(x - a) + b_{01}(y - b) \\ &+ 1/2(b_{20}(x - a)^2 + 2b_{11}(x - a)(y - b) + b_{02}(y - b)^2) \\ &+ \text{higher powers}\end{aligned}$$

Elliptic curve

Let us first consider the following example,

$$R = \mathbf{C}[x,y]/(\mathbf{f}(x,y)), \quad \mathbf{f}(x,y) = y^2 - x(x-1)(x-2).$$

By the Nullstellensatz its maximal ideals are of the form $M = (x-\alpha, y-\beta)$, where $\beta^2 - \alpha(\alpha-1)(\alpha-2) = 0$.
We claim that R_M is a PID. Write the polynomial $\mathbf{f}(x,y)$ as a combination of $x-\alpha$ and $y-\beta$

$$\begin{aligned} \mathbf{f}(x,y) &= A(x,y)(x-\alpha) + B(x,y)(y-\beta) \\ \frac{\partial \mathbf{f}}{\partial x}(\alpha,\beta) &= A(\alpha,\beta) \\ \frac{\partial \mathbf{f}}{\partial y}(\alpha,\beta) &= B(\alpha,\beta) \end{aligned}$$

Elliptic curve cont'd

If one of the partial derivatives is not zero at (α, β), in the ring R $\overline{A(x,y)}$ or $\overline{B(x,y)}$ are not in M, therefore one or the other is a unit in R_M so that the maximal ideal MR_M is generated by $\overline{y-\beta}$ or $\overline{x-\alpha}$:

$$\overline{\mathbf{f}(x,y)} = 0 = \overline{A(x,y)(x-\alpha)} + \overline{B(x,y)(y-\beta)}$$

It is easy to check that the conditions always holds since the partial derivatives are $2y$ and $(x-1)(x-x) + x(x-2) + x(x-1)$.

Volunteer please

Need someone to sketch the graph of the curve

$$y^2 = x(x-1)(x-2)$$

Geometric DD's

Let $\mathbf{f}(x, y) \in R = \mathbb{C}[x, y]$ be an irreducible polynomial. The algebraic variety

$$V(\mathbf{f}) = \{(a, b) \in \mathbb{C} : \mathbf{f}(a, b) = 0\}$$

is called a (plane) curve.

- We know that every maximal ideal of $\mathbb{C}[x, y]$ is of the form $M = (x - a, y - b)$, for $a, b \in \mathbb{C}$
- Thus if $\mathbf{f} \in M$ is a combination of the polynomials, $x - a$ and $y - b$, $\mathbf{f} = \mathbf{g}(x - a) + \mathbf{h}(y - b)$, so $\mathbf{f}(a, b) = 0$
- Conversely, if $\mathbf{f}(a, b) = 0$, writing the Taylor expansion of $\mathbf{f}(x, y)$ at $a, b)$ we get

$$\mathbf{f}(x, y) = \sum_{m+n \geq 0} a_{mn}(x - a)^m (y - b)^n, \quad a_{mn} \in \mathbb{C}$$

showing $\mathbf{f} \in (x - a, y - b)$.
- So points in $\mathbf{f} = 0$ and maximal ideals of $R/(\mathbf{f})$ correspond.

Let us determine when $R/(\mathbf{f})$ is a Dedekind domain. For that we define the ideal (Jacobian)

$$J(\mathbf{f}) = (\mathbf{f}, \frac{\partial \mathbf{f}}{\partial x}, \frac{\partial \mathbf{f}}{\partial y})$$

Theorem

$R/(\mathbf{f})$ is a Dedekind domain iff $J(\mathbf{f}) = (1)$.

Note what this means, if (a, b) is a point of the curve, $\mathbf{f}(a, b) = 0$, that is $\mathbf{f} \in M = (x - a, y - b)$, but because the ideal $J(\mathbf{f}) = (1)$, either $\frac{\partial \mathbf{f}}{\partial x}(a, b) \neq 0$ or $\frac{\partial \mathbf{f}}{\partial y}(a, b) \neq 0$. This means $\mathbf{f}(x, y) = 0$ has a tangent at (a, b).

Proof

- We are going to prove that for every maximal ideal M of $R = \mathbb{C}[x, y]/(\mathbf{f})$, R_M is a PID. For that, by a previous result, it will be enough to prove that the maximal ideal MR_M is principal.
- Since M is generated by the cosets of $x - a$ and $y - b$ for (a, b) such that $\mathbf{f}(a, b) = 0$, it will be enough to show that $x - a$ is a multiple of $y - b$ in R_M, or vice-versa.
- We are going to make use of the fact that one of the partial derivatives $\frac{\partial \mathbf{f}}{\partial x}(a, b)$ or $\frac{\partial \mathbf{f}}{\partial y}(a, b)$ is nonzero.

Proof cont'd

- Suppose $\frac{\partial \mathbf{f}}{\partial x}(a,b) \neq 0$. Let us write the Taylor expansion of $\mathbf{f}(x,y)$ at (a,b) (using that $\mathbf{f}(a,b) = 0$.
- We collect first the terms in which $x - a$ appears alone

$$(x-a)\underbrace{[\frac{\partial \mathbf{f}}{\partial x}(a,b) + 1/2 a_{2,0}(x-a) + \text{higher powers of } (x-a)]}$$

$$+(y-b)[\text{polynomial expression in } x-a \text{ and } y-b]$$

- Since this is the coset of $\mathbf{f}(x, y)$, it is zero.
- Note that the coefficient of $x - a$

$$\frac{\partial \mathbf{f}}{\partial x}(a, b) + 1/2a_{2,0}(x - a) + \text{higher powers of } (x - a)$$

  is a sum of an invertible element (the derivative) plus an element of MR_M, so it is an invertible element of R_M.
- This shows that $x - a$ is a multiple of $y - b$, and therefore MR_M is a principal ideal.

Creation of new D.D.'s

Theorem

Let R be a Dedekind domain of field of fractions $\mathbf{K}$ and let $\mathbf{L}$ a finite extension of $\mathbf{K}$. The integral closure $\mathbf{A}$ of R in $\mathbf{L}$ is a Dedekind domain.

The main burden is to show that $\mathbf{A}$ is a Noetherian ring. We will give a proof in case $\mathbf{L}$ is a separable extension, when one has that $\mathbf{A}$ is a finitely generated R-module. To get that we replace $\mathbf{L}$ by $\mathbf{M}$ its split closure over $\mathbf{K}$, and show that the integral closure $\mathbf{B}$ of R in $\mathbf{M}$ is a finitely generated R-module. Note that $\mathbf{A}$ is an R-submodule of $\mathbf{B}$.

Noetherianess of the integral closure

Theorem

Let R be an integrally closed Noetherian domain of field of fractions $\mathbf{K}$ and let $\mathbf{L}$ a finite Galois extension of $\mathbf{K}$. The integral closure $\mathbf{A}$ of R in $\mathbf{L}$ is a Noetherian domain.

Proof

- Let **G** be the Galois group of **L** over **K**. The **trace** is the function $u \in \mathbf{L} \to \mathbf{T}(u) = \sum_{\sigma \in \mathbf{G}} \sigma(u)$. Since the extension is Galois and $\mathbf{T}(u)$ is fixed by **G**, $\mathbf{T}(u) \in \mathbf{K}$.
- If u is integral over R, there is an equation $u^m + c_1 u^{m-1} + \cdots + c_m = 0$, with $c_i \in R$. Thus for any $\sigma \in \mathbf{G}$, $\sigma(u)$ is also integral over R and therefore $\mathbf{T}(u)$ is in **K** and integral over R, thus $\mathbf{T}(u) \in R$ since R is integrally closed.
- Define the quadratic form $\mathbf{S}(u, v) = \mathbf{T}(uv)$ on **L**. **S** is nondegenerate: If $u \neq 0$ we cannot have $\mathbf{T}(uv) = 0$ for all v, by the linear independence of automorphisms.

Proof cont'd

- Let $x_1, \ldots, x_n$ be a basis of **L** over **K**. By multiplying the x_i by nonzero elements of R we may assume that $x_i \in \mathbf{A}$.
- Let $y_1, \ldots, y_n$ be a basis of **L** dual to the x_i, that is $\mathbf{T}(x_i y_j) = \delta_{ij}$.
- For $u \in \mathbf{A}$, write $u = r_1 y_1 + \cdots + r_n y_n$. Then $\mathbf{T}(ux_i) = r_i \mathbf{T}(x_i y_i) = r_i$. Since $\mathbf{T}(ux_i) \in R$, this shows that **A** is contained in the finitely generated R-module $Ry_1 + \cdots + Ry_n$, and thus **A** is Noetherian as an R-module and hence a Noetherian ring as well.

Examples

- The most famous example obtained in this fashion is $\mathbb{Z}[i]$: Gaussian integers. It is the integral closure of $\mathbb{Z}$ in $\mathbf{Q}(i)$.
- The more general quadratic extension $\mathbf{Q}(\sqrt{m})$, m a squarefree integer is easy to examine. $z = a + b\sqrt{m}$, $a, b \in \mathbf{Q}$, is integral over $\mathbb{Z}$ iff $2a$ and $a^2 - b^2 m$ are integers. Thus a is an integer (and b is integer) or a is $1/2$ integer and b also a $1/2$ integer, depending on the residue class of m mod 4.
- If $m = 3$, $\mathbf{A} = \mathbb{Z}[\sqrt{3}]$; if $m = 5$, $\mathbf{A} = \mathbb{Z}[1/2 + 1/2\sqrt{5}]$; if $m = -5$, $\mathbf{A} = \mathbb{Z}[\sqrt{-5}]$.

Infinitely generated modules

Theorem

Let R be a DD. Then any submodule of a free module is a direct sum of ideals.

Done already. Recall the idea:

Proof. Let F be a free module with basis $\{e_i, i \in I\}$, and suppose the index set I is well-ordered. For each $i \in I$ set

$$F_i = \bigoplus_{j<i} Re_j,$$

with $F_0 = 0$ and $F_{i+1} = \bigoplus_{j \leq i} Re_j$.

For a submodule M of F each $x \in M \cap F_{i+1}$ has a unique expression $x = y + re_i$, where $y \in F_i$ and $r \in R$. If $\phi_i : M \cap F_{i+1} \to R$ is defined by $\phi_i(x) = r$, there is a SES

$$0 \to M \cap F_i \longrightarrow M \cap F_{i+1} \longrightarrow I_i \to 0,$$

where $I_i = \mathrm{image}\ \phi_i$.

To make the point clear, suppose

$$F = Re_1 \oplus \cdots \oplus Re_{n-1} \oplus Re_n = F' \oplus Re_n$$

gives $0 \to M \cap F' \longrightarrow M \longrightarrow I_n e_n \to 0$, and therefore $M \simeq I_n e_n \oplus M \cap F'$. Now use induction.
Same in general case: Since I_i is projective (as R is a D.D.), the sequence splits: $M \cap F_{i+1} = (M \cap F_i) \oplus C_i$, $C_i \simeq I_i$.
We claim $M = \bigoplus_i C_i$. Same proof from now on

Torsion and Torsionfree Modules

- Let R be an integral domain and M an R-module. The torsion submodule of M is the set

$$T(M) = \{x \in M : rx = 0, \quad 0 \neq r \in R\}$$

- $T(M)$ is a submodule of M. If $T(M) = M$, M is said to be a **torsion module**. If $T(M) = 0$, M is called **torsionfree**.
- $T(M/T(M)) = 0$, that is $M/T(M)$ is torsionfree.
- A set $\{x_1, \ldots, x_n\} \subset M$ is linearly independent if $\sum_i r_i x_i = 0$, $r_i \in R$, implies $r_i = 0$.
- The largest cardinality of the sets of linearly independent elements of M is the **torsionfree rank** of M.
- A nonzero ideal I of R has torsionfree rank 1: If $0 \neq x, y \in I$, $xy - yx = 0$ is a relation.

Proposition

If M is a finitely generated torsionfree module of rank n, then there is an embedding

$$M \hookrightarrow R^n.$$

Proof.

Let $M = (y_1, \ldots, y_m)$ and let $\{x_1, \ldots, x_n\}$ be a linearly independent set of elements of M.

For each y_j, we have a relation

$$c_j y_j + \sum_i a_{ij} x_i = 0, \quad c_j \neq 0$$

Let $c = \prod_j c_j$ and consider the elements $z_i = \frac{x_i}{c}$ of the module of fractions $c^{-1}M$. The z_i are linearly independent over R and each generator of M is contained in the free module

Structure of finitely generated modules

Theorem

Let R be a Dedekind domain and M a finitely generated R-module. Then

$$M \simeq T \oplus P,$$

where T is the torsion submodule of M and $P = M/T$ is a projective R-module. Moreover:

1. $P \simeq \underbrace{R \oplus \cdots \oplus R}_{\text{free}} \oplus I$, *where I is a unique ideal up to isomorphism.*
2. $T \simeq R/I_1 \oplus \cdots \oplus R/I_m$, $I_1 \subseteq \ldots \subseteq I_m$, *where the I_i are uniquely defined.*

Proof

- In the exact sequence $0 \to T \longrightarrow M \longrightarrow M/T \to 0$, $P = M/T$ is torsionfree, so embeds into a finitely generated free R-module (**why?**).
- P is projective, so the sequence splits: $M \simeq T \oplus P$.
- P we know is isomorphic to a direct of ideals. One improves this to a direct sum of a free and **one** ideal. This ideal is unique up to isomorphism. We will describe it later: it is called the **determinant** of the module M.
- T is actually a module over a PID S derived from R.

Outline

Homework

Assume R is a D.D.

1. Prove that for any two nonzero ideals I and J of R, $I \oplus J \simeq R \oplus IJ$.
2. Prove that any ideal I of a Dedekind domain can be generated by 1.5 elements, that is $I = (a, b)$, with a being any nonzero element.
3. Prove that any submodule of R^n is isomorphic to $R^r \oplus I$, for some ideal I.
4. (If we recall right) Prove that if M is a non-finitely generated submodule of a free module, then M is free.

Outline

Assignment #13

Do Problem #3 only

1. Let R be a D.D. and $P_1, \ldots, P_n$ a finite set of maximal ideals and U the complement of $\bigcup_i P_i$. Note that U is a multiplicative set. Prove that the ring of fractions $S = U^{-1}R$ is a D.D. with a finite number of maximal ideals.
2. If R is a D.D. and I is an ideal such that $P_1, \ldots, P_n$ are the prime ideals of $V(I)$, prove that for the ring of fractions S above, $R/I = S/IS$.
3. Prove that a D.D. with finitely many primes is a PID.
4. Prove that $\mathbb{R}[\cos t, \sin t]$ is a Dedekind domain.

Outline

Commutative Artinian Rings

Definition

The ring R is Artinian if it has the descending chain condition for ideals.

Besides fields, or finite rings, the simplest [yet not so simple] examples are algebras that are finite dimensional vector spaces over a field $\mathbf{K}$.

For non-commutative rings, this chain condition can be expressed in many forms [will explain later], but in the commutative case they just turn out to be a special type of Noetherian rings.

Elementary Properties

- Every prime ideal P of a commutative Artinian ring R is maximal: The quotient R/P is a domain so ETS Artinian domains are fields. If $a \neq 0$, the chain $(a) \supset (a^2) \supset \cdots$ stabilizes at $(a^n) = (a^{n+1})$, therefore $a^n = ra^{n+1}$ so $1 = ra$, since the ring is a domain.
- R has only a finite number of maximal ideals: Let $\{P_2, P_2, \ldots\}$ be distinct maximal ideals. Form the descending chain

$$P_1 \supset P_1 \cdot P_2 \supset P_1 \cdot P_2 \cdot P_3 \supset \cdots$$

that becomes stationary at

$$P_1 \cdot P_2 \cdots P_n = P_1 \cdot P_2 \cdots P_n \cdot P_{n+1}$$

Therefore P_{n+1} contains $P_1 \cdot P_2 \cdots P_n$, and thus $P_{n+1} = P_i$, $i \leq n$.

Jacobson Radical

Theorem

Let J be the intersection of all the maximal ideals of R. Then $J^n = 0$ for some integer n.

Proof.

Consider the descending chain $J \supset J^2 \supset \cdots$ that stabilizes at $J^n = J^{n+1}$. We claim that $J^n = 0$.

We argue by contradiction. Consider the set of nonzero ideals L such that $J^n L \neq 0$. Note that by assumption J is one such ideal. Choose a minimum ideal L with this property. Now, let $x \in L$ such that $J^n x \neq 0$. This shows $L = Rx$ by the minimality hypothesis and $x = ax$, $a \in J^n$. This implies $(1-a)x = 0$ and therefore $x = 0$ since $1 - a$ is invertible, a contradiction. □

Partition of the Unity

If R is a commutative ring, a partition of the unity is an special decomposition of the form

$$R = J_1 + \cdots + J_n, \quad J_i \text{ ideals of } R$$

Suppose $I_1, \ldots, I_n$ is a set of a ideals that is pairwise co-maximal, meaning $I_i + I_j = R$, for $i \neq j$. This obviously is a partition of the unikty.

Another arises from it [check!] if we set $J_i = \prod_{j \neq i} I_j$

$$R = J_1 + \cdots + J_n, \quad J_i \text{ ideals of } R$$

Chinese Remainder Theorem

Theorem

If I_i, $i \leq n$, is a family of ideals that is pairwise co-maximal, then for $I = I_1 \cap I_2 \cap \cdots \cap I_n$ there is an isomorphism

$$R/I \approx R/I_1 \times \cdots \times R/I_n.$$

Proof. Set $J_i = \prod_{j \neq I_j}$. Note that $I_i + J_i = R$. Since $J_1 + \cdots + J_n = R$, there is an equation

$$1 = a_1 + \cdots + a_n, \quad a_i \in J_i$$

Note that for each i, $a_i \cong 1 \mod I_i$. Define a mapping **h** from R to $R/I_1 \times \cdots \times R/I_n$, by $\mathbf{h}(x) = (\overline{xa_1}, \ldots, \overline{xa_n})$. We claim that **h** is a surjective homomorphism of kernel I.

Proof Cont'd

1. Since $a_i \cong 1 \mod I_i$,

$$\mathbf{h}(x) = (\overline{xa_1}, \dots, \overline{xa_n}) = (\overline{x}_1, \dots, \overline{x}_n)$$

which is clearly a homomorphism.

2. The kernel consists of the x such that $\overline{x}_i = 0$ for each i, that is $x \in I_i$ for each i–that is, $x \in I$.
3. To prove $\mathbf{h}$ surjective, for $u = (\overline{x_1}, \dots, \overline{x_n})$, setting

$$x = x_1 a_1 + \cdots + x_n a_n$$

gives $\mathbf{h}(x) = u$.

Structure of Artinian Rings

Theorem

Let R be a commutative Artinian ring, let $\{P_1, \ldots, P_n\}$ be the set of its maximal ideals, J its Jacobson radical and m an integer such that $J^m = 0$. Then

$$R \approx R/P_1^m \times \cdots \times R/P_n^m.$$

Moreover each R/P_i^m is Noetherian.

We apply CRT to the set of ideals $P_1^m, \ldots, P_n^m$ to obtain the decomposition. Now we must prove that each R/P_i^m is Noetherian.
Note that $S = R/P_i^m$ has a unique maximal ideal $M = P_i/P_i^m$, and that $M^m = 0$.

Proof Cont'd

1. Consider the chain of ideals $R \supset M \supset M^2 \supset M^{m-1} \supset M^m = 0$. To prove that R is Noetherian ETS each factor module M^i/M^{i+1} is Noetherian. [See last step]
2. We examine the factors M^i/M^{i+1}. This module is Artinian and is also annihilated by M. So it is actually an Artinian R/M-vector space, so must be finite dimensional, in particular it is a Noetherian module.
3. For example, suppose $M^3 = 0$. M^2 is annihilated by M, so it is a R/M-vector space, so it is also a Noetherian R-module.
4. Consider the exact sequence $0 \to M^2 \to M \to M/M^2 \to 0$. Both M^2 and M/M^2 are Noetherian, so M is Noetherian as well. The general case is similar.

Composition series

Theorem

If R is a commutative Artinian ring then there exists a tower of ideals

$$0 = M_0 \subset M_1 \subset \cdots \subset M_n = R$$

such that for all i, $M_i/M_{i-1} = R/P_i$ for some prime ideal P_i.

Proof. Left to reader.

Pop Quiz

Prove:

Theorem

Let $\mathbf{K}$ be a finite extension of $\mathbb{Q}$ and denote by $\mathbf{A}$ the integral closure of $\mathbb{Z}$ is $\mathbf{K}$. Then for every $0 \neq n \in \mathbb{Z}$, $\mathbf{A}/n\mathbf{A}$ is a finite ring.

Relate $|\mathbf{A}/n\mathbf{A}|$ to n and $\dim_{\mathbb{Q}} \mathbf{K}$.

Outline

Assignment #14

- Let R be a finitely generated algebra over the field $\mathbf{K}$ (that is, R is a homomorphic image of a polynomial ring in finitely many variables over $\mathbf{K}$). Prove that if R is Artinian, then $\dim_{\mathbf{K}} R < \infty$.