MA 252 notes: Commutative algebra

(Distilled from [Atiyah-MacDonald])

Dan Abramovich

Brown University

March 11, 2017

Unique factorization

Proposition

Let A be a noetherian domain of dimension 1, and $\mathfrak{a}$ an ideal. Then there is a unique factorization $\mathfrak{a} = \prod \mathfrak{q}_i$ where $\mathfrak{q}_i$ are primary and $r(\mathfrak{q}_i)$ distinct.

- Consider a minimal primary decomposition $\mathfrak{a} = \cap \mathfrak{q}_i$. Since $\dim A = 1$ we have $\mathfrak{p}_i$ maximal, hence pairwise coprime. So $\mathfrak{q}_i$ are pairwise coprime, so $\cap \mathfrak{q}_i = \prod \mathfrak{q}_i$.
- Uniqueness follows from the uniqueness of the primary decomposition, as all primes are isolated.

In case all primary ideals are prime powers, we have unique factorization into primes. We'll describe such rings.

Discrete valuation rings

- A discrete valuation on a field K is a surjective homomorphism $v : K^\times \to \mathbb{Z}$ such that $v(x+y) \geq \min(v(x), v(y))$.
- This implies that $\{0\} \cup \{x : v(x) \geq 0\}$ is a subring - the valuation ring. It is indeed a valuation ring of K.
- We have seen examples when we discussed valuations rings, we just need to define v: in $\mathbb{Z}_{(p)}$ or $\mathbb{Z}_p$ define $v(p) = 1$. In $k[x]_{(x)}$ or $k[\![x]\!]$ define $v(x) = 1$.
- A discrete valuation ring is the valuation ring of its fraction field. We have seen it is local, with maximal ideal $\mathfrak{m} = \{0\} \cup \{x : v(x) > 0\}$

Ideals in discrete valuation rings

- $v(x) = v(y)$ implies $(x) = (y)$.
- If $\mathfrak{a} \neq 0$ let $k = \min\{v(x) : x \in \mathfrak{a}\}$. Then $\mathfrak{a} = \{x : v(x) \geq k\} = \mathfrak{m}^k$.
- An element with $v(x) = 1$ generates $\mathfrak{m}$.
- It follows that the nonzero ideals are $\mathfrak{m}^k$, a single descending chain.
- Hence A noetherian.
- $\mathfrak{m}$ the only nonzero prime, hence $\dim A = 1$

Chracterizations of discrete valuation rings

Theorem

Let A be Noetherian local domain, $\dim A = 1$. Let $\mathfrak{m}$ maximal, $k = A/\mathfrak{m}$. We have equivalence:

(i) *A DVR*

(ii) *A integrally closed*

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

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

(v) *every nonzero ideal is $\mathfrak{m}^k$*

(vi) *there is x such that every nonzero ideal is (x^k).*

Chracterizations - proof...

A. Note that any $\mathfrak{a} \neq 0, 1$ is $\mathfrak{m}$-primary and contains some $\mathfrak{m}^n$ (proven for Noetherian)

B. Note that $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$ (since no $\mathfrak{m}^k = 0$).

- (i) implies (ii) since valuation ring.
- (iii) implies $\dim_k \mathfrak{m}/\mathfrak{m}^2 \leq 1$ by Nakayama, and equality from B, implying (iv).
- Assume (iv). Since $\mathfrak{a} \supset \mathfrak{m}^n$ we can apply what we learned in Artin rings and get that $\mathfrak{a}/\mathfrak{m}^n, \mathfrak{m}/\mathfrak{m}^n$ are principal, so $\mathfrak{a}/\mathfrak{m}^n = \mathfrak{m}^k/\mathfrak{m}^n$, implying (v).
- Take $x \in \mathfrak{m} \smallsetminus \mathfrak{m}^2$, so assuming (v), the ideal $(x) = \mathfrak{m}^k$ with $1 \leq k < 2$ and (vi) follows.
- Given (vi) we have $(x) = \mathfrak{m}$, and $(x^k) \neq (x^{k+1})$, so $a = \mu x^k$ for unique k and unit μ. Define $v(a) = k$ and extend $v(a/b) = v(a) - v(b)$. This defines a valuation... (i)

Chracterizations . . . proof end

- To prove (ii) implies (iii) take $0 \neq a \in \mathfrak{m}$.
- By (A), $\mathfrak{m}^n \subset (a)$ and $\mathfrak{m}^{n-1} \not\subset (a)$ for some n.
- Take $b \in \mathfrak{m}^{n-1} \setminus (a)$ and $x = a/b \in K$.
- $x^{-1} \notin A$ since $b \notin (a)$, so x^{-1} not integral over A.
- This implies $x^{-1}\mathfrak{m} \not\subset \mathfrak{m}$.
- Claim: $x^{-1}\mathfrak{m} = (b/a)\mathfrak{m} \subset A$. Indeed $(a) \supset \mathfrak{m}^n \supset \mathfrak{m}b$ implies $A \supset \mathfrak{m}\frac{b}{a}$
- So $x^{-1}\mathfrak{m} = A$, and $\mathfrak{m} = Ax = (x)$. ♠

Dedekind domains

Theorem

For A noetherian of dimension 1, the following are equivalent:

(i) *A integrally closed,*

(ii) *every primary ideal is a prime power,*

(iii) *every localization at a maximal ideal is a DVR.*

Such rings are called Dedekind domains.

- We have seen that being integrally closed is a local property, so (i) is equivalent to (iii). This is the key equivalence.
- If (ii) holds then in every $A_{\mathfrak{p}}$ every ideal is $\mathfrak{m}^k$ (by (A.)) so $A_{\mathfrak{p}}$ is DVR.
- Conversely, if $\mathfrak{a}$ is $\mathfrak{p}$-primary then $\mathfrak{a} \supset \mathfrak{p}^m$. We have $A_{\mathfrak{p}}/\mathfrak{m}^m \simeq A/\mathfrak{p}^m \supset \mathfrak{a}/\mathfrak{p}^m \simeq \mathfrak{a}_p/\mathfrak{m}^m$. If $A_{\mathfrak{p}}$ a DVR then $\mathfrak{a}_{\mathfrak{p}} = \mathfrak{m}^k$ so $\mathfrak{a}/\mathfrak{p}^m = \mathfrak{p}^k/\mathfrak{p}^m$ so $\mathfrak{a} = \mathfrak{p}^k$.

Unique factorization, rings of integers

Corollary

An ideal $\mathfrak{a} \neq 0$ in a Dedekind domain has a unique factorization $\mathfrak{a} = \prod \mathfrak{p}^k$ into prime powers.

Theorem

The ring of integers $\mathcal{O}_K$ in a number field K is a Dedekind domain.

- Noetherian: $K/\mathbb{Q}$ separable so $\mathcal{O}_K \subset \sum \mathbb{Z} v_i$. So A is a finitely generated $\mathbb{Z}$-module so Noetherian.
- Integrally closed: the integral closure is integrally closed.
- Dimension 1: Let $\mathfrak{p}$ be a nonzero prime. By the preliminaries to "going up" $\mathfrak{p} \cap \mathbb{Z} \neq 0$, so $\mathfrak{p} \cap \mathbb{Z} = (p)$ is maximal, so $\mathfrak{p}$ maximal.

Fractional ideals

- Fix a domain and fraction field $A \subset K$.
- A fractional ideal is an A-submidule $M \subset K$ such that for some $x \in K$ we have $xM \subset A$.
- Ideals are fractional ideals.
- Modules of the form Au are principal fractional ideals.
- If $M \subset K$ is a finitely generated A-module it is a fractional ideal, by clearing denominators of generators $x_i = y_i/z_i$.
- If A is noetherian and $M \subset K$ a fractional ideal then M is finitely generated: it is isomorphic to the ideal xM.

Invertible ideals

- An invertible ideal $M \subset K$ is such that there is $N \subset K$ with $MN = A$. In this case $N = (A : M) := \{x \in K : xM \subset A\}$: $N \subset (A : M) = (A : M)MN \subset AN = N$.
- An invertible ideal is finitely generated: if $M(A : M) = A$ then $\sum x_i y_i = 1, x_i \in M, y_i \in N$, so $x = \sum (y_i x)x_i$ with $y_i x \in A$.
- Invertible ideals form a group under multiplication,
- Nonzero principal fractional ideals form a subgroup.

Fractional ideals and localization

Proposition

If M fractional, these are equivalent:

- *M invertible,*
- *M finitely generated and $M_{\mathfrak{p}}$ invertible for all $\mathfrak{p}$,*
- *M finitely generated and $M_{\mathfrak{m}}$ invertible for all $\mathfrak{m}$.*

- If M invertible, then $A_{\mathfrak{p}} = (M(A : M))_{\mathfrak{p}} = M_{\mathfrak{p}}(A_{\mathfrak{p}} : M_{\mathfrak{p}})$, though you need to re-prove $(A : M)_{\mathfrak{p}} = (A_{\mathfrak{p}} : M_{\mathfrak{p}})$ in this context.
- If the last holds, write $\mathfrak{a} = M(A : M)$, an ideal. Again $\mathfrak{a}_{\mathfrak{m}} = M_{\mathfrak{m}}(A_{\mathfrak{m}} : M_{\mathfrak{m}}) = A_{\mathfrak{m}}$, so $\mathfrak{a} = A$.

Fractional ideals and DVRs

Proposition

A local is a DVR if and only if every nonzero fractional ideal is invertible.

- Assume A DVR and let $\mathfrak{m} = (x)$, $M \subset K$ fractional. There is $y \in A$ such that $yM \subset A$ so $yM = (x^r)$ so $M = (x^r/y)A$, in fact principal invertible of the form $x^{r-s}A$.
- If the fractional ideals are invertible, the ideals are invertible so finitely generated, and A noetherian. We claim every ideal is a power of $\mathfrak{m}$.
  The set of ideals which are not powers of $\mathfrak{m}$, if nonempty, have a maximal element $\mathfrak{a}$. Since $\mathfrak{a} \neq \mathfrak{m}$ we have $\mathfrak{a} \subset \mathfrak{m}$ and $\mathfrak{m}^{-1}\mathfrak{a} \subsetneq \mathfrak{m}^{-1}\mathfrak{m} = A$ an ideal containing $\mathfrak{a}$, so $\mathfrak{m}^{-1}\mathfrak{a} = \mathfrak{m}^k$ so $\mathfrak{a} = \mathfrak{m}^{k-1}$, contradiction.

Fractional ideals and Dedekind domains

Theorem

An integral domain A is a Dedekind domain if and only if every nonzero fractional ideal is invertible.

- Assume A Dedekind and $M \neq 0$ fractional. For all $\mathfrak{p} \neq 0$ we have $M_{\mathfrak{p}}$ fractional ideal in DVR $A_{\mathfrak{p}}$ so invertible. Also M finitely generated as A noetherian. It follows that M is invertible.
- Assume every fractional ideal is invertible. In particular every ideal is finitely generated so A noetherian. To show that all $A_{\mathfrak{p}}$ are DVRs it suffices by the previous result to show all ideals $\mathfrak{a}_{\mathfrak{p}}$ are invertible over $A_{\mathfrak{p}}$. But this follows since $\mathfrak{a}$ is invertible over A.

Ideal group and ideal class group

Corollary

For A Dedekind, nonzero fractional ideals form a group $\mathcal{I}(A)$ under multiplication.

The unit element is A.
We have an exact sequence $1 \to A^\times \to K^\times \to \mathcal{I}(A) \to Cl(A) \to 1$.

Corollary

A Dedekind domain A is a UFD if and only if it is a PID if and only if $Cl(A) = 1$.

Finiteness of the class group and the unit theorem

Theorem (Dirichlet)

Let K be a number field. Then $Cl(O_K)$ is finite.

Theorem (Dirichlet)

Let K be a number field. Then

$$O_K^\times \simeq \boldsymbol{\mu}(K) \times \mathbb{Z}^{r+s-1},$$

where the group $\boldsymbol{\mu}(K)$ of roots of 1 in K is ciclic, r is the number of distinct embeddings $K \hookrightarrow \mathbb{R}$, and $r + 2s = [K : \mathbb{Q}]$.

Affine algebraic curves

Theorem (Riemann, Abel-Jacobi)

Let A be the integral closure of $\mathbb{C}[x]$ in a finite extension K of $\mathbb{C}(x)$. Then there is an integer g such that

$$Cl(A) \simeq \mathbb{C}^g/\mathbb{Z}^{2g+t} \simeq (\mathbb{S}^1)^{2g}/\mathbb{Z}^t,$$

namely the subgroup $\mathbb{Z}^{2g+t}$ contains a lattice.
Also

$$A^\times \simeq \mathbb{C}^\times \times \mathbb{Z}^{t'}.$$

The integer $s = t + t' + 1$ counts the number of points needed to compactify the Riemann surface. It is bounded by $[K : \mathbb{C}(x)]$.
There is an exact sequence

$$1 \to \mathbb{C}^\times \to A^\times \to \mathbb{Z}^s \to (\mathbb{S}^1)^{2g} \times \mathbb{Z} \to Cl(A) \to 1.$$