MA4J8 Commutative algebra II

Week 1. Dedekind domains and prerequisites

1.1 Prerequisites

In the lectures, I dived into Dedekind domains at the deep end, and stepped back to discuss prerequisites (that most of the audience know perfectly well). The write-up lists some of the prerequisites first in more-or-less logical order. This is very boring, and you should start at Section 1.2. The material is intended to stand alongside the "frequently forgotten facts" (FFF) pages on the course website (and later prerequisite sections).

All rings here are commutative with a 1.

Integral domain and its field of fractions $K = \operatorname{Frac} A$. For the time being, we work with integral domains, so that the partial ring of fractions $S^{-1}A$ is a subset of the familiar construction of field of fractions, the set $\{\frac{a}{s} \mid a \in A, s \in S\}$. Later we use more general ring of fractions $S^{-1}A$, with S allowed to have zero divisors.

Principal ideal domain PID and unique factorisation domain UFD from Year 2 algebra.

Prime and maximal ideals $\operatorname{Spec} A$ is the set of primes of A. The subset of maximal ideals is m-$\operatorname{Spec} A$.

Local ring (A, m) The textbooks give equivalent definitions:

(i) A is a ring with a single maximal ideal m.

(ii) The set of nonunits of A is an ideal m.

(iii) m is a maximal ideal and $1 + x$ is a unit for all $x \in m$.

Zorn's lemma [UCA, 1.7]. This is the preferred version of the axiom of choice used by in algebra and most of set theory. It is comparable to the completeness axiom of the reals in Analysis courses, and could reasonably be described as completeness of set theory.

"Plenty of primes" [UCA, 1.9]. Zorn's lemma implies that given a proper ideal I and multiplicative set S in A, there exists an ideal P containing I and disjoint from S that is maximal with those conditions. This is prime. The statement that an ideal that is maximal among some specified class is prime is a repeating narrative of the subject.

Determinant trick or Cayley–Hamilton [UCA, 2.6-2.7] or [A&M, Prop 2.4] or [Ma, p.7] or [Eis, Th. 4.3]. An endomorphism φ of a finite A-module M satisfies a monic relation

$$\varphi^n + a_{n-1}\varphi^{n-1} + \cdots + a_1\varphi + a_0 = 0. \quad \text{with } a_i \in A. \tag{1.1}$$

Here n is the number of generators, and (1.1) is the characteristic polynomial $\det(\mathrm{Id}_M - \varphi) = 0$.

Integral extension Integral closure of A in a field L, definition of normal integral domain. An integral element b in L (or in an overring B of A) generates a finite ring extension $A[b]$, and a composition of finite extensions $A \subset B \subset C$ is finite by the same easy argument as in Galois theory, but to get the same result for integral extensions, and to get the result that the integral closure of A in L is a ring requires the Determinant trick. See [UCA, Chap. 4] or [A&M, Chap. 5] or [Ma, Chap. 3, Section 9].

Noetherian conditions on rings and modules. There are three equivalent conditions in the definition. To go from all submodules are f.g. or the a.c.c. to the maximal condition (every nonempty set of submodules has a maximal element) involves Zorn's Lemma.

Nakayama's lemma [UCA, 2.8 and Ex. 2.5] If A, m is a local ring and M a finite A-module then $mM = 0$ implies that $M = 0$. More general statement: if $M = IM$ for an ideal I and finite M then there exists an $x \in I$ with $x \equiv 1 \bmod I$ such that $xM = 0$.

Ann **and** Ass Let A be a ring and M an A-module. For nonzero $n \in M$, set $\mathrm{Ann}(n) = \{a \in A \mid an = 0\}$. It is obviously a proper ideal of A, the *annihilator ideal* of n.

An associated prime of M is a prime $P \in \operatorname{Spec} A$ such that $P = \mathrm{Ann}(n)$ for some $n \in M$. Equivalently, M contains a submodule isomorphic to the integral domain A/P. The set $\operatorname{Ass} M$ of associated primes of M plays a key role in many arguments.

Lemma 1.1 *An ideal that is maximal among* $\operatorname{Ann}(n)$ *is prime. Therefore* A *Noetherian and* $M \neq 0$ *implies* $\operatorname{Ass} M \neq \emptyset$.

Straightforward: if $fg \in \operatorname{Ann}(n)$ and $g \notin \operatorname{Ann}(n)$ then $f \in \operatorname{Ann}(gn) = \operatorname{Ann}(n)$ by the maximality of $\operatorname{Ann}(n)$. This is an instance of the "maximal in a class implies prime" narrative.

1.2 First view of Dedekind rings

Definition 1.2 (1) Let A be an integral domain with field of fractions $K = \operatorname{Frac} A$. For I a nonzero ideal of A, the *inverse* I^{-1} is the subset

$$I^{-1} = \{s \in K \mid sI \subset I\}. \tag{1.2}$$

You could say that I^{-1} consists of the common denominators of all $a \in I$.

(2) A nonzero ideal I of A is *invertible* if $I^{-1} \cdot I = A$.

(3) A is a *Dedekind domain* if every ideal I of A is invertible.

This is an extremely strong condition as we will shortly show. Dedekind domains are among the most important rings in pure math.

Exercise 1.3 (1) If ideal I is f.g., prove that $I^{-1} \neq 0$.

(2) (Harder) Give an example of A, I such that $I^{-1} = 0$.

(3) Let $M_1, M_2 \subset K$ be nonzero A-submodules of K. Prove that any A-linear map $\varphi\colon M_1 \to M_2$ is multiplication by some $s \in K$.

(4) Show that $I^{-1} = \operatorname{Hom}_A(I, A)$.

Lemma 1.4 *An invertible ideal* I *is finitely generated. Therefore a Dedekind domain is a Noetherian ring*

Proof Since $I^{-1} \cdot I = A$, there exists an expression

$$1 = \sum s_i a_i \quad \text{with } s_i \in I^{-1} \text{ and } a_i \in I. \tag{1.3}$$

This is a finite sum. Now for every $x \in I$,

$$x = 1 \cdot x = \sum (s_i x) a_i \tag{1.4}$$

so I is generated by the finitely many a_i. For the second part, every ideal of A is f.g., one of the equivalents definitions of Noetherian. (See the prerequisites. The equivalence of the definitions needs Zorn's lemma.)

Definition 1.5 The *localisation* of an integral domain A at a prime ideal P is

$$A_P = \{a/s \in K \mid a, s \in A, s \notin P\}. \tag{1.5}$$

This is a subring of K, and it is a local ring with maximal ideal PA_P. In fact, an element $a/s \in A_P$ for which $a \notin P$ has inverse $s/a \in A_P$, so the nonunits of A_P consist of the ideal PA_P.

Exercise 1.6 (1) See the equivalent definitions of local ring in the prerequisites, and make you understand why they are equivalent.

(2) Maximal ideals $m_1 \neq m_2$ have $m_1 + m_2 = A$ and $m_1 \cap m_2 = m_1 m_2$.

Lemma 1.7 *If A is a Dedekind domain and I a nonzero ideal then the ideal IA_P is principal for every $P \in \operatorname{Spec} A$.*

Proof As above, $\sum s_i a_i = 1 \in A$. Now $1 \notin P$, so at least one of them (say with $i = 0$) has $s_0 a_0 \notin P$. Hence

$$u = s_0 a_0 = \tfrac{s_0 a_0}{1} \quad \text{is a unit of } PA_P. \tag{1.6}$$

Therefore $a_0 \in I$ generates IA_P. In fact,

$$ux = (s_0 x) a_0 \quad \text{for any } x \in I. \tag{1.7}$$

Here u is a unit of A_P and $s_0 x \in A$.

Exercise 1.8 Prove the following:

(1) Any ideal I of a Dedekind domain A is generated by at most 2 elements.

(2) Any two distinct prime ideals of A satisfy $P_1 + P_2 = A$.

(3) Any nonzero $x \in A$ is only contained in finitely many ideals.

(4) If I is an ideal of A with $(a_1, \ldots, a_k)$, and $(s_1, \ldots, s_k)$ as in (1.3) the surjective map $\pi\colon A^{\oplus k} \to I$ that takes the ith basis element e_i to a_i has a right inverse (or "lift") s with $\pi \circ s = \mathrm{Id}_I$. Deduce that I is isomorphic to a direct summand of the free module $A^{\oplus k}$. See [Ma, Th. 11.3, p. 80] and compare later treatment of projective modules.

I will treat DVRs a bit later, so this is a bit out of order. For integral closure, see the prerequisite section.

Corollary 1.9 *Let A be a Dedekind domain and $P \in \operatorname{Spec} A$ a nonzero prime ideal. Then the localisation (A_P, PA_P) is a DVR. For $P = 0$, obviously $A_P = K = \operatorname{Frac} A$.*

In fact by the lemma, A_P is a Noetherian local ring and its maximal ideal PA_P is principal. This is one of the simple definitions of DVR.

Proposition 1.10 *A Dedekind ring A is normal. That is, any element of $x \in K = \operatorname{Frac} A$ that is integral over A (satisfies a monic polynomial equation over A) is already an element of A.*

Proof Suppose that x is integral over A. Then x satisfies a monic dependence relation over A, and the same relation is also a monic relation over A_P for every $P \in \operatorname{Spec} A$. On the other hand A_P is a DVR, hence a UFD, and so $x \in A_P$. Therefore x is contained in the intersection of A_P taken over every $P \in \operatorname{Spec} A$.

However, this intersection is A itself. Proof [UCA, 8.7 Lemma]. Write $D = \{d \in A \mid dx \in A \subset A$ (the set of all possible denominators of x, and 0). This is an ideal of A. If $D \neq A$ then D is a proper ideal, so is contained in a maximal ideal P of A, so that $x \notin A_P$. $\square$

The converse is also true, but the argument is longer. I prove the following Main Theorem below (mainly following [Ma, Theorem 11.6, p. 82]).

Theorem 1.11 (Characterisation of Dedekind domains) *Let A be an integral domain. Equivalent conditions:*

(1) *A is a Dedekind domain.*

(2) *A is one dimensional normal Noetherian domain.*

(3) *A is Noetherian and its localisation at every nonzero prime ideal is a DVR.*

(4) *Every nonzero ideal of A can be written as a product $\prod_i p_i^{s_i}$ of a finite number of powers of prime ideals.*

Moreover, the factorisation in (4) *is unique.*

1.3 Characterisation of DVRs

The baby definition is UFD with single prime element $z \in A$, so that every element of A is $z^v u$ with a a unit. This is equivalent to Noetherian integral domain, that is a local ring A, m with principal maximal ideal $m = (z)$. It is also equivalent to the conditions that the field of fractions $K = \operatorname{Frac} A$ has a valuation $v\colon K \twoheadrightarrow \mathbb{Z} \sqcup \{\infty\}$ (a multiplicative homomorphism on $K^\times$ s.t. $v(f+g) \geq \min(v(f), v(g))$) such that $A = \{x \in K \mid v(x) \geq 0\}$ and $m = \{x \in K \mid v(x) > 0\}$. Exercise: prove equivalence.

So far, this is quite straightforward. The main result goes in a more abstract direction:

Theorem 1.12 *A is a DVR if and only it is a Noetherian integral domain that is local with exactly two prime ideals $\{0, m\}$ (in other words, has Krull dimension 1), and is normal (integrally closed in $K = \operatorname{Frac} A$).*

Local integral domain means that 0 and m are prime. $\operatorname{Spec} A = \{0, m\}$ gives no prime ideals strictly between 0 and m (so Krull dimension 1). Now A is Noetherian, so the ideal m is f.g., and Nakayama's lemma implies that $m \neq m^2$.

Claim 1.13 *Any $x \in m \setminus m^2$ generates m.*

The assumption that $m/(x) \neq 0$ leads to a contradiction. For this we need the notion of associate prime, that is an important point for the rest of the course. By Lemma 1.1 of the above prerequisite section, $m/(x) \neq 0$ would imply that $\operatorname{Ass}(m/(x)) \neq \emptyset$, and therefore $m/(x)$ must contain a submodule isomorphic to A/P for some $P \in \operatorname{Spec} A$.

However $\operatorname{Spec} A$ only has 2 elements 0 and m, and 0 certainly doesn't work so that (still working by contradiction), we can assume $m \in \operatorname{Ass}(m/(x))$, and $m/(x)$ contains a nonzero element $\overline{y}$ killed by m. Lifting $\overline{y}$ to $y \in m$ gives an element $y \in m \setminus (x)$ so that $m \cdot y \subset x$. Now $x, y \in A$, so that y/x is an element of $K = \operatorname{Frac} A$ satisfying $y/x \notin A$ but $m \cdot y/x \in A$.

Two possible cases:

(i) $m \cdot (y/x) = A$.

(ii) $m \cdot (y/x) \subset m$.

The first case gives $1 \in m \cdot (y/x)$, with implies at once that $x \in m \cdot y$, which contradicts the assumption in the claim that $x \notin m^2$.

So far, we have not used the assumption of the Main Theorem that A is normal. In case (ii), the contradiction arises by applying the Cayley–Hamilton result to the A-linear homomorphism $\varphi\colon m \to m$ given by multiplication by y/x. This gives a monic relation for y/x

$$(y/x)^n + a_{n-1}(y/x)^{n-1} + \cdots + a_1(y/x) + a_0 = 0.$$

with coefficients in A. The relation holds as an endomorphism of m as A-module, but everything takes place inside the field K, so that the relation proves that y/x is integral over A. Since A is normal, this implies that $y/x \in A$, or $y \in (x)$, which contradicts $y \in m \setminus (x)$. This proves the claim and the Main Theorem.

```
The characterisation of Dedekind domains is similar --
Noetherian, 1-dimension and integrally closed implies Dedekind.

I leave the proof as exc. for now. See Exc. 1.8.
```

1.4 Dedekind and Weber's synthesis

Dedekind domains include the ring of integers $\mathcal{O}_K$ of a number field K, and the coordinate ring $k[C]$ of a nonsingular affine curve C. These objects are main protagonists of algebraic number theory and algebraic geometry, and are clearly very different in nature. However, Dedekind and Weber [DW] say that these two rings can be studied using the same algebraic apparatus. They are rarely UFDs, but (informally) can invariably be treated as UFDs "away from finitely many primes".

The good news: if A is a ring of either type (a Dedekind domain), the ideals of A have *unique factorisation into prime ideals.*

1.5 Modern abstract algebra

The 1882 paper Dedekind and Weber [DW] marks a breakthrough: modern algebra has axioms and abstract arguments, and often works with objects in a symbolic way. In this case, without reference to what the elements of the ring actually are. At bit later in the century, Cayley wrote several essays on groups, emphasising that the important thing about them was the mechanism of composing group elements, not the nature of the *operators* making up the group.

[DW] Richard Dedekind and Heinrich Weber, Theorie der algebraischen Funktionen einer Veränderlichen, J. reine angew. Math. **92** (1882), 181–290

1.6 Essay on organisation

Algebra has a logical development (definition, assertion, proof) but it also has meaning (examples, applications, thought experiments, history, everything else). The problem with the logical or "pure thought" approach is that it does not indicate the eventual aim, and that it frequently does not say what is nontrivial and important. If you concentrate only on the logic, you spend too much time worrying about tautologies, and lose out on everything else. The logic is not necessarily memorable, and rarely suggests the next step forward.

This course is a second course in commutative algebra, and has prerequisites at many levels. The student (and not infrequently the lecturer) needs timely reminders rather than a full rigorous treatment. I summarise these by keeping a list of FFF Frequently Forgotten Facts (but I have probably missed some items). Life is complicated, and its logical ordering is the least of our worries.