Chapter 2 : Commutative algebra

Broadly speaking commutative algebra is the study of commutative rings (with identity). It constitutes the basic building block for some other areas of mathematics like algebraic geometry and algebraic number theory. In fact the 'local' approach in these branches of mathematics owes a great deal to commutative algebra or more precisely to the study of the prime spectra of rings. However, for this course I plan to remain more 'global' than 'local' (for the sake of simplicity!) and this immediately reduces the requirements in the usage of commutative algebra tools. Nonetheless, some concepts from commutative algebra will be deployed in the rest of the course and it is expedient to compile these concepts in a convenient form. Of course, my selection of topics in this chapter needed for the global treatment of number fields and number rings would fail to provide the reader the proper flavor of commutative algebra. That does not matter, in particular, in a one-semester course with rather modest requirements on the part of the participants.

Once again let me iterate that within the framework of this course a `ring` always means a *commutative ring with identity*. Also a ring homomorphism $A \to B$ is always assumed to map 1_A to 1_B.

2.1 Localization

I planned to stay global and still start with localization. Don't worry! You may perhaps read the section heading as 'Rings of fractions'. I will not very deeply discuss the local issues in rings of fractions.

The concept of formation of fractions of integers to give the rationals can be applied in a more general setup. Instead of having any non-zero element in the denominator of a fraction we may allow only elements from a specific subset. All we require to make the collection of fractions a ring is that the allowed denominators should be closed under multiplication. This leads us to the following definition:

2.1 Definition Let A be a ring. A non-empty subset S of A is called `multiplicatively closed` or simply `multiplicative`, if $1 \in S$ and for any $s, t \in S$ we have $st \in S$.

2.2 Example (1) For a non-zero ring A the subset $A \setminus \{0\}$ is multiplicatively closed, if and only if A is an integral domain. For a general non-zero ring A the set of all elements $a \in A$ such that a is not a zero-divisor is a multiplicative subset of A.

(2) Let A be a ring and $\mathfrak{a}$ a proper ideal of A. Then the set $A \setminus \mathfrak{a}$ is multiplicatively closed, if and only if $\mathfrak{a}$ is a prime ideal of A.

(3) For a ring A and an element $f \in A$ the set $\{1, f, f^2, f^3, \ldots\} \subseteq A$ is multiplicatively closed.

Let A be a ring and S a multiplicative subset of A. We define a relation $\sim$ on $A \times S$ as $(a, s) \sim (b, t)$, if and only if $u(at - bs) = 0$ for some $u \in S$. (If A is an integral domain, one may take $u = 1$ in the definition of $\sim$.) It is easy to check that $\sim$ is an equivalence relation on $A \times S$. The set of equivalence classes of $A \times S$ under $\sim$ is denoted by $S^{-1}A$, whereas the equivalence class of $(a, s) \in A \times S$ is denoted as a/s (instead of as $[(a, s)]$). For $a/s, b/t \in S^{-1}A$ define $(a/s) + (b/t) := (at + bs)/(st)$ and $(a/s)(b/t) := (ab)/(st)$. It is easy to check that these operations are well-defined and make $S^{-1}A$ a ring with identity $1/1$, in which each $s/1$, $s \in S$, is invertible. There is a canonical ring homomorphism $\imath : A \to S^{-1}A$ taking $a \mapsto a/1$. In general, $\imath$ is *not* injective. However, if A is an integral domain and $0 \notin S$, then the injectivity of $\imath$ can be proved easily (Exercise 2.1.2) and we say that the ring A is canonically embedded in the ring $S^{-1}A$.

2.3 Definition Let A be a ring and S a multiplicative subset of A. The ring $S^{-1}A$ constructed as above is called the `localization of` A `away from` S or the `ring of fractions` of A with respect to S.

2.4 Example (1) Let A be an integral domain and let $S = A \setminus \{0\}$. Then $S^{-1}A$ is called the quotient field or the field of fractions of A and is denoted as $\mathrm{Q}(A)$. If A is already a field, then $\mathrm{Q}(A) \cong A$. Other examples include $\mathrm{Q}(\mathbb{Z}) = \mathbb{Q}$ and $\mathrm{Q}(K[X]) = K(X)$, K a field, where $K(X)$ denotes the field of rational functions over K in one indeterminate X.

More generally, if A is any ring and S is the set of all non-zero-divisors of A, then $S^{-1}A$ is called the total quotient ring of A and is again denoted by $\mathrm{Q}(A)$. It is, in general, not a field. If A is an integral domain, then $S = A \setminus \{0\}$ and the usage of $\mathrm{Q}(A)$ remains consistent.

(2) Let A be a ring, $\mathfrak{p}$ a prime ideal of A and $S := A \setminus \mathfrak{p}$. Then $S^{-1}A$ is called the localization of A at $\mathfrak{p}$ and is usually denoted by $A_{\mathfrak{p}}$.

(3) Let A be a ring, $f \in A$ and $S = \{1, f, f^2, f^3, \ldots\}$. In this case $S^{-1}A$ is conventionally denoted by A_f.

This example illustrates a typical way of exploiting the use of different scripts for designating different kinds of objects. Having said nothing else, it becomes questionable how to distinguish between the meanings of $A_{\mathfrak{p}}$ and A_f. But our convention is to use Gothic letters (like $\mathfrak{p}$) for ideals and italicized Roman letters (like f) for elements of rings (and some other things too, but for these other things no object with the notation A_f is defined). This should remove all confusions that may crop up while using similar notations for two different (and yet similar) kinds of things.

It is important to look at the prime ideals in rings of fractions (though it leads us to the local zone). For a treatment of general ideals in localizations we refer the reader to Exercise 2.1.4.

2.5 Proposition Let A be a non-zero ring, S a multiplicative subset of A and $B := S^{-1}A$. Then the prime ideals of B are in one-to-one inclusion-preserving correspondence with the prime ideals of A that do not meet S.

Proof Let P_1 denote the set of prime ideals of B and P_2 the set of prime ideals of A that do not meet S. We first define a map $f : P_1 \to P_2$ by $\mathfrak{P} \mapsto \mathfrak{p} := \imath^{-1}(\mathfrak{P})$, where $\imath : A \to B$ is the canonical ring homomorphism. Clearly $\mathfrak{p}$ is a prime ideal of A (since for any ring homomorphism the inverse image of a prime ideal is always prime). In order to show that $\mathfrak{p}$ does not meet S (i.e., f is well-defined), we assume otherwise, i.e., let $s \in \mathfrak{p} \cap S$. Since $\imath(\mathfrak{p}) = \imath(\imath^{-1}(\mathfrak{P})) \subseteq \mathfrak{P}$, it follows that $s/1 \in \mathfrak{P}$. But $s/1$ is a unit in B and hence $\mathfrak{P}$ is the unit ideal, a contradiction.

Conversely, we define a map $g : P_2 \to P_1$ by $\mathfrak{p} \mapsto \mathfrak{P} := S^{-1}\mathfrak{p} := \{a/b \mid a \in \mathfrak{p}, b \in S\}$. Clearly $\mathfrak{P}$ is an ideal of B. We claim that $\mathfrak{P}$ is a proper ideal of B, for if not, $a/b = 1/1$ for some $a \in \mathfrak{p}$ and $b \in S$. But then $u(a - b) = 0$ for some $u \in S$. Since $\mathfrak{p} \cap S = \emptyset$, it follows that $u \notin \mathfrak{p}$ and $a - b \notin \mathfrak{p}$, but their product (i.e., 0) is in $\mathfrak{p}$, a contradiction to the fact that $\mathfrak{p}$ is prime. Now let $a/b, c/d \notin \mathfrak{P}$, i.e., $a, c \notin \mathfrak{p}$ and $b, d \in S$. Since $\mathfrak{p}$ is prime, $ac \notin \mathfrak{p}$, and since S is multiplicatively closed, $bd \in S$. One can then check that $(a/b)(c/d) = (ac)/(bd) \notin \mathfrak{P}$. Thus $\mathfrak{P}$ is a prime ideal of B, i.e., g is well-defined.

Checking that f and g are inverses of one another is left to the reader as an easy exercise. It is also clear that this correspondence is inclusion-preserving. ◀

All number rings are instances of a particular kind of rings known as Dedekind domains in which non-zero ideals admit unique factorization (in some sense). One possible way to define Dedekind domains is to use the theory of localizations. This is, however, the local definition. We will later provide a global definition and prove that these two definitions are actually equivalent. We start by giving a series of definitions.

2.6 Definition A (non-zero) ring A with a unique maximal ideal $\mathfrak{m}$ is called a local ring. In that case the field $A/\mathfrak{m}$ is called the residue field of A.

The next example gives a justification for these terms.

2.7 Example Let A be ring and $\mathfrak{p}$ a prime ideal of A. It follows from Proposition 2.5 that the localization $A_\mathfrak{p}$ is a local ring with the unique maximal ideal $\mathfrak{p}A_\mathfrak{p}$ generated by elements a/b, $a \in \mathfrak{p}$, $b \notin \mathfrak{p}$. The residue field $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ is canonically isomorphic to the quotient field $\mathrm{Q}(A/\mathfrak{p})$ of the integral domain $A/\mathfrak{p}$ under the ring homomorphism $(a/b) + \mathfrak{p}A_\mathfrak{p} \mapsto (a+\mathfrak{p})/(b+\mathfrak{p})$, $a \in A$, $b \in A \setminus \mathfrak{p}$. In particular, if $\mathfrak{m}$ is a maximal ideal of A, then the fields $A/\mathfrak{m}$ and $A_\mathfrak{m}/\mathfrak{m}A_\mathfrak{m}$ are isomorphic.

2.8 Definition A ring A is called a discrete valuation ring (DVR) or a discrete valuation domain (DVD), if A is a local principal ideal domain.

Some immediate properties of DVRs are explored in Exercise 2.1.7. Let me now furnish the local definition of Dedekind domains. Unfortunately, however, I have to use a term – 'Noetherian' – that is not defined yet. In Section 3 of this chapter we will see three equivalent ways of defining a Noetherian ring.

2.9 Definition A ring A is called a Dedekind domain, if A is a Noetherian integral domain such that the localization $A_\mathfrak{p}$ is a DVR for every non-zero prime ideal $\mathfrak{p}$ of A.

I will, however, make little use of Definition 2.9 while dealing with number rings. It's, however, not a bad idea to tell the readers the different avenues to reach the same location.

Exercises for Section 2.1

1. Let A be a ring and S a multiplicatively closed subset of A. Show that if $0 \in S$, then $S^{-1}A$ is the zero ring.

2. Let A be a ring, $S \subseteq A$ multiplicative and $\imath : A \to S^{-1}A$ the canonical ring homomorphism $a \mapsto a/1$. Show that:
(a) $\imath(s)$ is invertible in $S^{-1}A$ for every $s \in S$.
(b) $\imath(a) = 0$, if and only if $as = 0$ for some $s \in S$.
(c) $\imath$ is injective, if and only if S is contained in the set of non-zero-divisors of A.

3. [Universal property of rings of fractions] Let A, S and $\imath$ be as in Exercise 2.1.2. Further suppose that $\varphi : A \to B$ is a ring homomorphism such that $\varphi(s) \in B^*$ for all $s \in S$. Show that there exists a unique ring homomorphism $\psi : S^{-1}A \to B$ satisfying $\varphi = \psi \circ \imath$.

4. Let A be a ring, S a multiplicative subset of A, $B := S^{-1}A$ and $\imath : A \to B$ the canonical homomorphism. For any subset T of A we use the notation $S^{-1}T := \{t/s \mid s \in S, t \in T\}$.
(a) Let $\mathfrak{a}$ be an ideal of A. Show that the extended ideal $\mathfrak{a}^e$ in B is the ideal $S^{-1}\mathfrak{a}$.
(b) Show that every ideal in B is an extended ideal.

5. Let A be a ring (not necessarily an integral domain) and let $\mathrm{Q}(A)$ denote (as usual) the total quotient ring of A. Show that every element of $\mathrm{Q}(A)$ is either a zero-divisor or a unit.

6. A multiplicative subset S of a ring A is called saturated, if $ab \in S$ (with $a, b \in A$) implies that $a \in S$ and $b \in S$. Show that S is a saturated multiplicative subset of A, if and only if $A \setminus S$ is a union of prime ideals (of A). (**Hint:** For proving the "only if" part let P denote the set of all prime ideals of A contained in $A \setminus S$. One can show that $A \setminus S = \bigcup_{\mathfrak{p} \in P} \mathfrak{p}$ as follows. Clearly $\bigcup_{\mathfrak{p} \in P} \mathfrak{p} \subseteq A \setminus S$. For the converse take any $x \in A \setminus S$. First show that $x/1$ is not a unit is $S^{-1}A$. Then $x/1$ is contained in a maximal ideal $S^{-1}\mathfrak{p}$ of $S^{-1}A$ for some $\mathfrak{p} \in P$. Prove that $x \in \mathfrak{p}$.)

7. Let A be a DVR with maximal ideal $\mathfrak{m} = \langle p \rangle$. Prove the following assertions:
(a) A is a UFD.
(b) The only primes in A are the associates of p. (**Hint:** In a PID non-zero prime ideals are maximal.)
(c) Every non-zero element of A can be written as up^α, where u is a unit of A and $\alpha \in \mathbb{Z}_+$.
(d) Every non-zero ideal of A is of the form $\langle p^\alpha \rangle$ for some $\alpha \in \mathbb{Z}_+$.

(e) A has only one non-zero prime ideal (namely, $\mathfrak{m}$).

(**Remark:** The prime p of A is called a uniformizing parameter or a uniformizer for A and is unique up to multiplication by units.

The map $\nu : A \setminus \{0\} \to \mathbb{Z}_+$ taking $up^\alpha \mapsto \alpha$ is called a discrete valuation of A and can be naturally extended to a group homomorphism $\nu : K^* \to \mathbb{Z}$ by defining $\nu(a/b) := \nu(a) - \nu(b)$, where $a, b \in A$, $b \neq 0$ and $K = \mathrm{Q}(A)$ is the quotient field of A. It is often convenient to define $\nu(0) := +\infty$. It follows that $A = \{x \in K \mid \nu(x) \geqslant 0\}$ and $\mathfrak{m} = \{x \in K \mid \nu(x) > 0\}$.)

8. [Polynomial rings over a UFD] Let A be a UFD and $K := \mathrm{Q}(A)$.

(a) Show that every non-zero $f(X) \in K[X]$ can be written as $f(X) = \alpha f_1(X)$ for some $\alpha \in K^*$ and for some primitive polynomial $f_1(X) \in A[X]$. Show further that α and f_1 are uniquely determined by f up to multiplication by units of A.

(b) Let $f(X) \in A[X]$ be a non-constant polynomial. Prove that f is irreducible over A, if and only if f is irreducible over K. (**Hint:** Use Part (a) and Exercise 1.1.5.) In particular, the irreducible elements of $A[X]$ are those of A and the primitive polynomials in $A[X]$ that are irreducible in $K[X]$.

*** (c)** Deduce that $A[X]$ is a UFD and so also are the domains $A[X_1, \ldots, X_n]$ for all $n \in \mathbb{N}$.

2.2 Integral dependence

The concept of integral dependence is at the heart of defining the number rings in an attempt to generalize the notion of 'integers'. Recall that if $K \subseteq L$ is a field extension, then an element $\alpha \in L$ is called algebraic over K, if α is a root of a non-zero polynomial $f \in K[X]$. Since K is a field, the polynomial f can be divided by its leading coefficient, thereby giving a *monic* polynomial in $K[X]$ of which α is a root. However, if K and L are general rings (i.e., not fields), division by the leading coefficient is not always permissible. This leads us to the following definition.

2.10 Definition Let $A \subseteq B$ be an extension of rings. An element $\alpha \in B$ is said to be integral over A, if α satisfies[1] (i.e., is a root of) a *monic* (and hence non-zero) polynomial $f \in A[X]$. An equation of the form $f(\alpha) = 0$, $f \in A[X]$ monic, is called an equation of integral dependence of α over A.

2.11 Example (1) If both A and B are fields, the concepts of "integral" and "algebraic" elements are the same. (See the argument preceding Definition 2.10.)

(2) Take $A := \mathbb{Z}$ and $B := \mathbb{Q}$ and let $a/b \in \mathbb{Q}$, $\gcd(a, b) = 1$, be integral over $\mathbb{Z}$. Let $(a/b)^n + \alpha_{n-1}(a/b)^{n-1} + \cdots + \alpha_1(a/b) + \alpha_0$, $\alpha_i \in \mathbb{Z}$, be an equation of integral dependence of a/b over $\mathbb{Z}$. Multiplication by b^n gives $a^n = -b(\alpha_{n-1}a^{n-1} + \cdots + \alpha_1 ab^{n-2} + \alpha_0 b^{n-1})$, i.e., $b \mid a^n$. Since $\gcd(a, b) = 1$, this forces $b = \pm 1$, i.e., $a/b \in \mathbb{Z}$. This is, in general, true for any UFD A and its field of fractions $B = \mathrm{Q}(A)$ (See Exercise 2.2.1).

(3) Every element $\alpha \in A$ is integral over A, since it satisfies the monic polynomial $X - \alpha \in A[X]$.

Now let $A \subseteq B$ be an extension of rings and let C consist of all the elements of B that are integral over A. Clearly $A \subseteq C \subseteq B$. But what algebraic structure does C actually have? It turns out that C is again a ring. This result is not at all immediate from the definition of integral elements. We prove this fact by using the following lemma which sort of generalizes Theorem 1.62.

[1] Strictly speaking α being a root of $f(X)$ is equivalent to α satisfying the polynomial *equation* $f(\alpha) = 0$. But often the term 'equation' is dropped in this context – a harmless colloquial contraction.

2.12 Lemma For a ring extension $A \subseteq B$ and for $\alpha \in B$ the following conditions are equivalent:

(a) α is integral over A.

(b) $A[\alpha]$ is a finitely generated A-module.

(c) $A[\alpha] \subseteq C$ for some subring C of B with C being a finitely generated A-module.

Proof [(a)⇒(b)] Let $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$, $a_i \in A$, be an equation of integral dependence of α over A. $A[\alpha] = \{f(\alpha) \mid f(X) \in A[X]\}$ is generated as an A-module by $1, \alpha, \alpha^2, \ldots$. In order to show that only the elements $1, \alpha, \ldots, \alpha^{n-1}$ generate $A[\alpha]$ as an A-module, it is sufficient to show that each α^k, $k \in \mathbb{Z}_+$, is an A-linear combination of $1, \alpha, \ldots, \alpha^{n-1}$. We proceed by induction on k. The assertion certainly holds for $k = 0, \ldots, n-1$, whereas for $k \geqslant n$ we write $\alpha^k = -(a_{n-1}\alpha^{k-1} + \cdots + a_1\alpha^{k-n+1} + a_0\alpha^{k-n})$, whence induction completes the proof.

[(b)⇒(c)] Take $C := A[\alpha]$.

[(c)⇒(a)] Let $\gamma_1, \ldots, \gamma_n \in C$ generate C as an A-module. Since $A[\alpha] \subseteq C$ and, in particular, $\alpha \in C$, for all $i = 1, \ldots, n$ we can write $\alpha\gamma_i = \sum_{j=1}^n a_{ij}\gamma_j$ for some $a_{ij} \in A$. Let $\mathfrak{A}$ denote the matrix $(\alpha\delta_{ij} - a_{ij})_{1 \leqslant i,j \leqslant n}$, where δ_{ij} is the Kronecker delta. Then $\mathfrak{A}(\gamma_1, \ldots, \gamma_n)^{\mathrm{t}} = (0, \ldots, 0)^{\mathrm{t}}$. Multiplication (on the left) by the adjoint of $\mathfrak{A}$ shows that $(\det \mathfrak{A})\gamma_i = 0$ for all $i = 1, \ldots, n$. Since $1 \in C$, we have $1 = \sum_{i=1}^n b_i\gamma_i$ for some $b_i \in A$, so that $(\det \mathfrak{A}) \cdot 1 = 0$, i.e., $\det \mathfrak{A} = 0$. But $\det \mathfrak{A}$ is a monic polynomial in α of degree n and with coefficients from A. ◀

2.13 Proposition For an extension $A \subseteq B$ of rings the set

$$C := \{\alpha \in B \mid \alpha \text{ is integral over } A\}$$

is a subring of B containing A.

Proof Clearly $A \subseteq C \subseteq B$ as sets. To show that C is a ring let $\alpha, \beta \in C$. By Condition (b) of Lemma 2.12 $A[\alpha]$ is a finitely generated A-module. Now β being integral over A is also integral over $A[\alpha]$, so that again by 2.12(b) $A[\alpha][\beta]$ is a finitely generated $A[\alpha]$-module. It is then easy to check that $A[\alpha, \beta] = A[\alpha][\beta]$ is a finitely generated A-module. Since $\alpha \pm \beta$ and $\alpha\beta$ are in $A[\alpha, \beta]$, by condition 2.12(c) these elements are integral over A, i.e., belong to C. Thus C is a ring. ◀

This proposition leads us to the following important definitions.

2.14 Definition The ring C of Proposition 2.13 is called the integral closure of A in B. A is called integrally closed in B, if $C = A$. On the other hand, if $C = B$, we say that B is an integral extension of A or that B is integral over A.

An integral domain A is called integrally closed (without specific mention of the ring in which it is so), if A is integrally closed in its quotient field $\mathrm{Q}(A)$. An integrally closed integral domain is sometimes also termed a normal domain (ND).

2.15 Example (1) $\mathbb{Z}$ (or more generally any UFD) is an ND.

(2) $\mathbb{Z}$ is not integrally closed in $\mathbb{R}$ or $\mathbb{C}$, since, for example, $\sqrt{2} \in \mathbb{R}\backslash\mathbb{Z}$ is integral over $\mathbb{Z}$. The integral closure of $\mathbb{Z}$ in $\mathbb{C}$ is often denoted by $\mathbb{A}$. Elements of $\mathbb{A}$ are called algebraic integers. (See Exercise 1.4.8.)

After much ado we are finally in a position to define the basic objects of study in this course.

2.16 Definition A number field K is defined to be a finite (and hence algebraic) extension of the field $\mathbb{Q}$ of rational numbers. Clearly $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ with $[K : \mathbb{Q}]$ finite.

Note that there exist considerable controversies among mathematicians in accepting this definition of number fields. Some insist that any field K satisfying $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ should be called a number field. Some others restrict the definition by further demanding that one must have K *algebraic* over $\mathbb{Q}$. However, the fields K with infinite extension degree $[K : \mathbb{Q}]$ are allowed. We restrict the definition further by imposing the condition that $[K : \mathbb{Q}]$ has to be finite. Our restricted definition is seemingly the most widely accepted one. Whether or not this is the case is rather immaterial. We will study only the number fields of Definition 2.16 and accepting this definition would at the minimum save us from writing huge expressions like 'algebraic number fields of finite extension degree over $\mathbb{Q}$' to denote 'number fields'.

For number fields the notion of integral closure leads to the following definition.

2.17 Definition Let K be a number field. Then K contains $\mathbb{Q}$ and hence $\mathbb{Z}$. The integral closure of $\mathbb{Z}$ in K is called the ring of integers of K and is denoted by $\mathfrak{O}_K$. ($\mathfrak{O}$ is the Gothic 'O'.) Clearly $\mathbb{Z} \subseteq \mathfrak{O}_K \subseteq K$ and $\mathfrak{O}_K$ is an integral domain. We also have $\mathfrak{O}_K = \mathbb{A} \cap K$. A number ring is a ring which is (isomorphic to) the ring of integers of a number field.

Other notations commonly used for $\mathfrak{O}_K$ are $\mathbb{Z}_K$ and $\mathcal{O}_K$, where $\mathcal{O}$ is the upper case 'O' in the calligraphic script. The use of the letter 'O' is attributed to Gauss who coined the term *order* to denote some related objects. Students may use any of the notations $\mathfrak{O}_K$, $\mathbb{Z}_K$ or $\mathcal{O}_K$ interchangeably to denote number rings. But if one deals with curves (like elliptic curves), the point at infinity is also denoted by $\mathcal{O}$. It is, therefore, safer to avoid using the calligraphic style $\mathcal{O}_K$ in the context of number rings.

By Example 2.11(2) the ring of integers of the number field $\mathbb{Q}$ is $\mathbb{Z}$, i.e., $\mathfrak{O}_{\mathbb{Q}} = \mathbb{Z}$. It is, therefore, customary to call the elements of $\mathbb{Z}$ rational integers. Since $\mathbb{Z}$ is naturally embedded in $\mathfrak{O}_K$ for any number field K, it is important to notice the distinction between the integers of K (i.e., the elements of $\mathfrak{O}_K$) and the rational integers of K (i.e., the images of the canonical inclusion $\mathbb{Z} \hookrightarrow K$).

Some simple properties of number rings are listed below.

2.18 Proposition Let K be a number field. Then the following statements hold:

(1) $\mathfrak{O}_K \cap \mathbb{Q} = \mathbb{Z}$.

(2) For $\alpha \in K$ there exists a rational integer $a \in \mathbb{Z}$ such that $a\alpha \in \mathfrak{O}_K$. In particular, the quotient field of $\mathfrak{O}_K$ is K.

(3) $\mathfrak{O}_K$ is integrally closed in $K = \mathrm{Q}(\mathfrak{O}_K)$, i.e., $\mathfrak{O}_K$ is a normal domain.

Proof (1) follows immediately from Example 2.11(2). (2) follows from Exercise 1.4.8 of Chapter 1. Finally (3) follows from Exercise 2.2.2(b). ◀

The rest of the course is devoted to investigating some other properties of the number rings $\mathfrak{O}_K$. Let us now continue our study of commutative algebra.

Exercises for Section 2.2

1. Show that every UFD is an ND. (**Hint:** Imitate the case of $\mathbb{Z}$ as described in Example 2.11(2).)

2. **(a)** If $A \subseteq B$ and $B \subseteq C$ are integral extensions of rings, show that $A \subseteq C$ is also an integral extension.
(b) Let $A \subseteq B$ be an extension of rings. Show that the integral closure of A in B is integrally closed in B.

(c) Let $A \subseteq B$ be an integral extension of rings, $\mathfrak{b}$ an ideal of B and $\mathfrak{a} := A \cap \mathfrak{b}$. (Note that $\mathfrak{a}$ is an ideal of A. Moreover, if $\mathfrak{b}$ is prime in B, then $\mathfrak{a}$ is also prime in A.) Show that $B/\mathfrak{b}$ is an integral extension of $A/\mathfrak{a}$.

3. Let $A \subseteq B$ be an extension of integral domains, $\mathfrak{a}$ a finitely generated non-zero ideal of A and $\gamma \in B$. If $\gamma\mathfrak{a} \subseteq \mathfrak{a}$, show that γ is integral over A. (**Hint:** Let $\mathfrak{a} = Ax_1 + \cdots + Ax_n$, $x_i \in \mathfrak{a}$. For each i write $\gamma x_i = \sum_{j=1}^{n} a_{ij}x_j$, $a_{ij} \in A$. But then $\det \mathfrak{A} = 0$, where $\mathfrak{A} = (\gamma\delta_{ij} - a_{ij})_{1 \leqslant i,j \leqslant n}$, δ_{ij} being the Kronecker delta.)

4. (a) Let $A \subseteq B$ be an integral extension of integral domains. Show that A is a field, if and only if B is a field.

(b) Let $A \subseteq B$ be an integral extension of rings, $\mathfrak{q}$ a prime ideal of B and $\mathfrak{p} := A \cap \mathfrak{q}$. Show that $\mathfrak{p}$ is maximal in A, if and only if $\mathfrak{q}$ is maximal in B. (**Hint:** Use (a) and Exercise 2.2.2(c).)

(c) Let A, B, $\mathfrak{p}$ and $\mathfrak{q}$ be as in (b). Further let $\mathfrak{q}'$ be another prime ideal of B with $\mathfrak{p} = A \cap \mathfrak{q}'$. Show that if $\mathfrak{q} \subseteq \mathfrak{q}'$, then $\mathfrak{q} = \mathfrak{q}'$. (**Hint:** Let $S := A \setminus \mathfrak{p}$. By Exercise 2.2.5 below $B_{\mathfrak{p}} := S^{-1}B$ is integral over $A_{\mathfrak{p}} = S^{-1}A$. Let $\mathfrak{m}$ be the ideal generated by $\mathfrak{p}$ in $A_{\mathfrak{p}}$ and let $\mathfrak{n}$ and $\mathfrak{n}'$ be the ideals of $B_{\mathfrak{p}}$ generated respectively by $\mathfrak{q}$ and $\mathfrak{q}'$. Now use Part (b).)

5. Let $A \subseteq B$ be a ring extension and let C be the integral closure of A in B. Show that for any multiplicative set S of A (and hence of B and C) the integral closure of $S^{-1}A$ in $S^{-1}B$ is $S^{-1}C$. In particular, if A is integrally closed in B, then so is $S^{-1}A$ in $S^{-1}B$.

6. Let A be an integral domain. Show that the following conditions are equivalent:
(1) A is integrally closed.
(2) $A_{\mathfrak{p}}$ is integrally closed for every prime ideal $\mathfrak{p}$ of A.
(3) $A_{\mathfrak{m}}$ is integrally closed for every maximal ideal $\mathfrak{m}$ of A.
(**Hint:** For proving "(1)⇒(2)" use Exercise 2.2.5. For proving "(3)⇒(1)" show first that $A = \bigcap_{\mathfrak{m} \in \operatorname{Spm} A} A_{\mathfrak{m}}$.)

7. A quadratic number field is a number field K with $[K : \mathbb{Q}] = 2$.

(a) Show that every quadratic number field K can be represented as $K \cong \mathbb{Q}(\sqrt{D})$ for a *square-free* integer $D \neq 0, 1$.

*** (b)** Let $K := \mathbb{Q}(\sqrt{D})$ for some square-free integer $D \neq 0, 1$. Show that:

$$\mathfrak{O}_K \cong \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] \cong \mathbb{Z}[X]/\langle X^2 - X + \frac{1-D}{4}\rangle & \text{if } D \equiv 1 \pmod 4, \\ \mathbb{Z}[\sqrt{D}\,] \cong \mathbb{Z}[X]/\langle X^2 - D\rangle & \text{if } D \equiv 2, 3 \pmod 4. \end{cases}$$

(In particular, the ring of integers of $\mathbb{Q}(\mathrm{i}) = \{a + \mathrm{i}b \mid a, b \in \mathbb{Q}\}$ is the ring $\mathbb{Z}[\mathrm{i}] = \{a + \mathrm{i}b \mid a, b \in \mathbb{Z}\}$ of Gaussian integers.)

2.3 Noetherian rings

Recall that a PID is a ring (integral domain) in which every ideal is principal, i.e., generated by a single element. We may now be a bit more general and demand every ideal to be finitely generated. If a ring meets our demand, we call it a Noetherian ring. As we now see, there are other equivalent ways of defining Noetherian rings. These rings are named after Emmy Noether (1882–1935) who was one of the most celebrated lady mathematicians of all ages and whose work on Noetherian rings has been very fundamental and deep in the branch of algebra. Emmy's father Max Noether (1844–1921) was also an eminent mathematician.

2.19 Definition Let A be a ring and let $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \cdots$ be an ascending chain of ideals of A. This chain is called stationary, if there is an $n \in \mathbb{N}$ such that $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \mathfrak{a}_{n+2} = \cdots$. The ring A is said to satisfy the ascending chain condition or the ACC, if every ascending chain of ideals in A is stationary, or in other words, if there does not exist any infinite strictly ascending chain $\mathfrak{a}_1 \subsetneqq \mathfrak{a}_2 \subsetneqq \mathfrak{a}_3 \subsetneqq \cdots$ of ideals in A.

2.20 Proposition For a ring A the following conditions are equivalent:

(a) Every ideal of A is finitely generated.

(b) A satisfies the ascending chain condition.

(c) Every non-empty set of ideals of A contains a maximal element.

Proof [(a)⇒(b)] Let $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots$ be an ascending chain of ideals of A. Consider the ideal $\mathfrak{a} := \bigcup_{n\in\mathbb{N}} \mathfrak{a}_n$ which is finitely generated by hypothesis. Let $a_1, \ldots, a_r$ be a set of generators of $\mathfrak{a}$. Each $a_i \in \mathfrak{a}$, i.e., there exists $m_i \in \mathbb{N}$ such that $a_i \in \mathfrak{a}_{m_i}$ and hence $a_i \in \mathfrak{a}_n$ for every $n \geqslant m_i$. Take $m := \max(m_1, \ldots, m_r)$. Then for every $n \geqslant m$ we have $\mathfrak{a} \subseteq \mathfrak{a}_n$, i.e., $\mathfrak{a} = \mathfrak{a}_n$.

[(b)⇒(c)] Let S be a non-empty set of ideals of A. Order S by inclusion. The ACC implies that every chain in S has an upper bound in S. By Zorn's lemma S has a maximal element.

[(c)⇒(a)] Let $\mathfrak{a}$ be an ideal of A. Consider the set S of all finitely generated ideals of A contained in $\mathfrak{a}$. S is non-empty, since it contains the zero ideal. By condition (c) S has a maximal element, say, $\mathfrak{b}$. If $\mathfrak{b} \subsetneqq \mathfrak{a}$, take $a \in \mathfrak{a} \setminus \mathfrak{b}$. Then $\mathfrak{b} + \langle a\rangle$ is finitely generated (since $\mathfrak{b}$ is so), properly contains $\mathfrak{b}$ and is contained in $\mathfrak{a}$. This contradicts the maximality of $\mathfrak{b}$ in S. Thus we must have $\mathfrak{a} = \mathfrak{b}$, i.e., $\mathfrak{a}$ is finitely generated. ◀

2.21 Definition A ring A is called Noetherian, if A satisfies (one and hence all of) the equivalent conditions of Proposition 2.20.

2.22 Example (1) All PIDs are Noetherian, since principal ideals are obviously finitely generated. In particular, $\mathbb{Z}$ and $K[X]$ (K a field) are Noetherian.

(2) If A is Noetherian and $\mathfrak{a}$ an ideal of A, then $A/\mathfrak{a}$ is Noetherian, since the ideals of $A/\mathfrak{a}$ are in one-to-one inclusion-preserving correspondence with the ideals of A containing $\mathfrak{a}$ and hence satisfy the ACC.

(3) Let A be a Noetherian ring and S a multiplicative subset of A. Then the localization $B := S^{-1}A$ is also Noetherian. To prove this fact let $\mathfrak{b}$ be an ideal in B. By Exercise 2.1.4(b) $\mathfrak{b} = S^{-1}\mathfrak{a}$ for some ideal $\mathfrak{a}$ of A. Since A is Noetherian, $\mathfrak{a}$ is finitely generated, say, $\mathfrak{a} = \langle a_1, \ldots, a_r\rangle$. It is now (almost) obvious that $\mathfrak{b}$ is generated by $a_1/1, \ldots, a_r/1$. A particular case is that if A is Noetherian and $\mathfrak{p}$ a prime ideal of A, then the localization $A_\mathfrak{p}$ is also Noetherian.

(4) We will later prove that all number rings $\mathfrak{O}_K$ are Noetherian.

(5) The ring $A := \mathbb{Z}[X_1, X_2, X_3, \ldots]$ of polynomials with infinitely many indeterminates $X_1, X_2, X_3, \ldots$ is not Noetherian. This is because the ideal $\langle X_1, X_2, X_3, \ldots\rangle$ is not finitely generated, or alternatively because we can produce the infinite strictly ascending chain of ideals: $\langle X_1\rangle \subsetneqq \langle X_1, X_2\rangle \subsetneqq \langle X_1, X_2, X_3\rangle \subsetneqq \cdots$, or because the set $S := \{\langle X_1\rangle, \langle X_1, X_2\rangle, \langle X_1, X_2, X_3\rangle, \ldots\}$ of ideals in A does not contain a maximal element.

In a similar manner one may define the descending chain condition (DCC) on ideals. A ring satisfying the DCC is called Artinian (after Emil Artin). An Artinian ring is always Noetherian, but not conversely. We will not study Artinian rings in this course.

We have seen that if A is a PID, the polynomial ring $A[X]$ need not be a PID. However, the property of being Noetherian is preserved during the passage from A to $A[X]$.

2.23 Theorem [Hilbert's basis theorem] If A is a Noetherian ring, then so is the polynomial ring $A[X_1, \ldots, X_n]$ for $n \in \mathbb{N}$. In particular, the rings $\mathbb{Z}[X_1, \ldots, X_n]$ and $K[X_1, \ldots, X_n]$ are Noetherian, where K is a field.

Proof Using induction on n and the fact that $A[X_1, \ldots, X_n] = A[X_1, \ldots, X_{n-1}][X_n]$ we can reduce the proof to the case of $n = 1$, that is, it is sufficient to prove that if A is Noetherian, then $A[X]$ is also

Noetherian. Let $\mathfrak{a}$ be a non-zero ideal of $A[X]$. Assume that $\mathfrak{a}$ is not finitely generated. Then we can inductively choose non-zero polynomials $f_1, f_2, f_3, \ldots$ from $\mathfrak{a}$ such that for each $i \in \mathbb{N}$ the polynomial f_i is one having the smallest degree in $\mathfrak{a} \setminus \langle f_1, \ldots, f_{i-1}\rangle$. Let $d_i := \deg f_i$. Then $d_1 \leqslant d_2 \leqslant d_3 \leqslant \cdots$. Let a_i denote the leading coefficient of f_i. Consider the ideal $\mathfrak{b} := \langle a_i \mid i \in \mathbb{N}\rangle$ in A. By hypothesis $\mathfrak{b}$ is finitely generated, say, $\mathfrak{b} = \langle a_1, \ldots, a_r\rangle$. This, in particular, implies that $a_{r+1} = \sum_{i=1}^{r} \gamma_i a_i$ for some $\gamma_i \in A$. But then the polynomial $g := f_{r+1} - \sum_{i=1}^{r} \gamma_i X^{d_{r+1}-d_i} f_i$ belongs to $\mathfrak{a}\setminus\langle f_1, \ldots, f_r\rangle$ (since $f_{r+1} \notin \langle f_1, \ldots, f_r\rangle$), is non-zero, in particular, and has degree $< d_{r+1}$, a contradiction to the choice of f_{r+1}. Thus $\mathfrak{a}$ must be finitely generated. ◀

Now we give an alternative definition of Dedekind domains.

2.24 Definition An integral domain A is called a Dedekind domain, if it satisfies *all* of the following three conditions:

(1) A is Noetherian.

(2) Every *non-zero* prime ideal of A is maximal.

(3) A is integrally closed (in its quotient field $K := \mathrm{Q}(A)$).

I will now show that the two definitions 2.9 and 2.24 are equivalent. But before this is done, we need to distinguish between the two classes of rings introduced in these two definitions. Let us call a Dedekind domain as per Definition 2.9 a DD_1 and a Dedekind domain as per Definition 2.24 a DD_2.

2.25 Proposition Let A be a ring which is not a field. Then A is a DD_1, if and only if A is a DD_2.

Proving this proposition requires the following lemma.

2.26 Lemma Let A be a local Noetherian integral domain which is not a field. Assume further that the maximal ideal $\mathfrak{m} \neq 0$ of A is the only non-zero prime ideal of A. Then A is a DVR (i.e., a PID), if and only if A is integrally closed.

Proof [if] Choose any $a \in \mathfrak{m}$, $a \neq 0$. For each $b \in A$ the set $\mathfrak{a}_b := \{r \in A \mid rb \in Aa\}$ is an ideal of A containing the ideal Aa. Since A is Noetherian, the (non-empty) set $S := \{\mathfrak{a}_b \mid b \notin Aa\}$ has a maximal element, say $\mathfrak{a}_c$ (Proposition 2.20). Then $\mathfrak{a}_c \neq 0$, since $\mathfrak{a}_c$ contains the non-zero ideal Aa. Also $\mathfrak{a}_c \neq A$, since $1 \notin \mathfrak{a}_c$. Now let $xy \in \mathfrak{a}_c$ with $x \notin \mathfrak{a}_c$. Then $xc \notin Aa$ and $\mathfrak{a}_{xc} \in S$ contains both $\mathfrak{a}_c$ and y. By the maximality of $\mathfrak{a}_c$ in S we then have $y \in \mathfrak{a}_c$. Thus $\mathfrak{a}_c$ is prime and hence, by hypothesis, $\mathfrak{a}_c = \mathfrak{m}$, i.e., $\mathfrak{m}c \subseteq Aa$. This, in turn, implies that each cx, $x \in \mathfrak{m}$, is a multiple of a. Then $(c/a)\mathfrak{m} = \{(c/a)x \mid x \in \mathfrak{m}\} \subseteq A$ is an ideal of A. We claim that $(c/a)\mathfrak{m} = A$. For the proof assume otherwise, i.e., $(c/a)\mathfrak{m} \subseteq \mathfrak{m}$. A is Noetherian and so by Exercise 2.2.3 c/a is integral over A. By hypothesis A is integrally closed, so that $c/a \in A$, i.e., $c \in Aa$, a contradiction. Thus $(c/a)\mathfrak{m} = A$, i.e., $(c/a)\alpha = 1$ for some $\alpha \in \mathfrak{m}$, i.e., $\mathfrak{m} = A\alpha$ is principal.

Now let $\mathfrak{a}$ be a non-zero ideal of A. Consider the chain $\mathfrak{a} \subseteq (1/\alpha)\mathfrak{a} \subseteq (1/\alpha^2)\mathfrak{a} \subseteq \cdots$ of subsets of $\mathrm{Q}(A)$. Assume that $(1/\alpha^k)\mathfrak{a}$ is a subset (and hence an ideal) of A for each $k \in \mathbb{Z}_+$. Since A is Noetherian, the chain must be stationary, i.e., $(1/\alpha^k)\mathfrak{a} = (1/\alpha^{k+1})\mathfrak{a}$ for some k, i.e., $(1/\alpha)\mathfrak{a} = \mathfrak{a}$. Once again by Exercise 2.2.3 this implies that $1/\alpha = c/a$ is integral over A, a contradiction. Thus, for some $k \in \mathbb{Z}_+$ we have $(1/\alpha^k)\mathfrak{a} \subseteq A$, but $(1/\alpha^{k+1})\mathfrak{a} \not\subseteq A$. If $(1/\alpha^k)\mathfrak{a}$ is a proper ideal of A, then $(1/\alpha^k)\mathfrak{a} \subseteq \mathfrak{m} = A\alpha$, i.e., $(1/\alpha^{k+1})\mathfrak{a} \subseteq A$, a contradiction. Therefore, $(1/\alpha^k)\mathfrak{a} = A$, i.e., $\mathfrak{a} = A\alpha^k$, i.e., $\mathfrak{a}$ is principal.

[only if] A UFD (in particular, a PID) is integrally closed. ◀

Proof of Proposition 2.25 [if] Let $\mathfrak{p} \neq 0$ be a prime ideal of A. Then $A_{\mathfrak{p}}$ is clearly a Noetherian local integral domain and is integrally closed by Exercise 2.2.6. Moreover, since each non-zero prime ideal of A is maximal, $\mathfrak{p}A_{\mathfrak{p}}$ is the only non-zero prime ideal of $A_{\mathfrak{p}}$. Then by Lemma 2.26 $A_{\mathfrak{p}}$ is a DVR.

[only if] That A is Noetherian follows from definition of DD_1. In order to show that A is integrally closed we use Exercise 2.2.6 and the fact that for each non-zero prime ideal $\mathfrak{p}$ of A the localization $A_{\mathfrak{p}}$ is a DVR (by definition of DD_1) and hence is integrally closed (A PID is a UFD.). Finally let $\mathfrak{p}$ be a non-zero prime ideal of A. $\mathfrak{p}$ is contained in a maximal (and hence prime) ideal $\mathfrak{p}'$ of A. By the correspondence of Proposition 2.5 $\mathfrak{p}A_{\mathfrak{p}'} \subseteq \mathfrak{p}'A_{\mathfrak{p}'}$ are prime ideals of $A_{\mathfrak{p}'}$. By definition $A_{\mathfrak{p}'}$ is a DVR and hence contains a unique non-zero prime ideal (Exercise 2.1.7). This implies that $\mathfrak{p}A_{\mathfrak{p}'} = \mathfrak{p}'A_{\mathfrak{p}'}$, i.e., $\mathfrak{p} = \mathfrak{p}'$. ◀

Henceforth, we will use the abbreviation DD to stand for Dedekind domain. Thus DD, DD_1 and DD_2 are now the same concepts.

Exercises for Section 2.3

1. Let $A \subseteq B$ be an extension of rings. Prove or disprove:

(a) If A is Noetherian, then B is necessarily Noetherian.

(b) If B is Noetherian, then A is necessarily Noetherian.

2. Let B be a finitely generated A-algebra. Prove or disprove:

(a) If A is Noetherian, then B is necessarily Noetherian.

*** (b)** If B is Noetherian, then A is necessarily Noetherian.

3. Let A be a ring with the property that every non-empty set of *finitely generated* ideals of A has a maximal element. Show that A is Noetherian.

4. **(a)** Let A be a Noetherian ring, $\mathfrak{a}$ an ideal of A and $\mathfrak{b} := \sqrt{\mathfrak{a}}$. Show that $\mathfrak{a} \supseteq \mathfrak{b}^m$ for some $m \in \mathbb{N}$. (**Hint:** Let $\mathfrak{b} = \langle b_1, \ldots, b_r \rangle$ and let $b_i^{m_i} \in \mathfrak{a}$, $m_i \in \mathbb{N}$. You may take any $m \geqslant 1 + \sum_{i=1}^{r}(m_i - 1)$.)

(b) Demonstrate by an example that the result of Part (a) does not necessarily hold, if A is not Noetherian.

5. Let A be a Dedekind domain and S a multiplicative subset of A. Show that $S^{-1}A$ is also a Dedekind domain. (**Hint:** Every prime ideal of $S^{-1}A$ is of the form $S^{-1}\mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal of A (that does not meet S). Verify that $A_{\mathfrak{p}} \cong (S^{-1}A)_{S^{-1}\mathfrak{p}}$ and then use Definition 2.9.)

6. Let A be a Dedekind domain.

(a) Let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be two distinct non-zero prime ideals of A. Show that for any $e_1, e_2 \in \mathbb{N}$ we have $\mathfrak{p}_1^{e_1} + \mathfrak{p}_2^{e_2} = A$. (**Hint:** Since $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are maximal, we have $\mathfrak{p}_1 + \mathfrak{p}_2 = A$, i.e., $a_1 + a_2 = 1$ for some $a_1 \in \mathfrak{p}_1$ and $a_2 \in \mathfrak{p}_2$. Now use the fact that $(a_1 + a_2)^{e_1+e_2} = 1$.)

(b) Let $\mathfrak{a} := \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ be a non-zero ideal of A with pairwise distinct prime ideals $\mathfrak{p}_i$ and with $e_i \in \mathbb{N}$. Show that $A/\mathfrak{a} \cong \prod_{i=1}^{r}(A/\mathfrak{p}_i^{e_i})$. (**Hint:** Use the CRT and Exercise 1.2.2.)