Notes on Chapter 1 of Dedekind's *Theory of Algebraic Integers*

1 Algebraic background

Recall that in a **commutative ring** $\langle R, 0, 1, +, \times \rangle$,

- $\langle R, 0, + \rangle$ is an abelian group,
- $\langle R - \{0\}, 1, \times \rangle$ is an abelian semigroup, and
- multiplication distributes over addition.

The same structure is a **field** if, in the second clause, $\langle R - \{0\}, 1, \times \rangle$, is a group; in other words, every nonzero element has an inverse.

A **vector space** V over a field F is an abelian group $\langle V, 0, + \rangle$ with an operation of "scalar multiplication" by elements of F, satisfying

- $a(bv) = (ab)v$
- $a(v + w) = av + aw$
- $(a + b)v = av + bv$
- $1v = v$

Here a and b are any elements of F, v and w are any elements of V, and 1 is the unit element of the field. The definition of a **module** M over a ring R is exactly the same, replacing V and F by M and R, respectively. In other words, a vector space is just a special case of a module, where the ring in question happens to be a field.

You should be familiar with a number of important facts about vector spaces from elementary linear algebra. For example, a **basis** for a vector space is a linearly independent set that spans the space. Every vector space has a basis, and any two bases have the same cardinality. For finite dimensional vector spaces (that is, spaces with a finite basis), any linearly independent set of the right size is a basis. Linear transformations from one finite dimensional vector space to another can be represented by a **matrix**, and the transformation is invertible if and only if the **determinant** of the associated matrix is nonzero.

Many of these notions carry over to modules, but the situation is more delicate. For example, there are modules, even finitely generated ones, that do not have bases; and even if a module has a finite basis, it is not necessarily the case that all bases are the same size, nor the case that any independent set of the right size can serve as a basis. For example, both $\mathbb{Z}_m$ (the integers mod m, under addition) and $\mathbb{Z}$ can be interpreted as $\mathbb{Z}$-modules (see below), but the first has no basis, even though it is generated by the set $\{1\}$; $\{1\}$ can serve as a basis for the second, but the set $\{2\}$ cannot.

A module with a basis is called a **free** module. As is the case with vector spaces, a free R-module with a basis of n elements looks just like n copies of R, $R \times R \times \ldots \times R$. Every R-module $\mathfrak{m}$ can be written as a quotient $\mathfrak{b}/\mathfrak{a}$, where $\mathfrak{b}$ is a free R-module, and $\mathfrak{a}$ is an appropriate submodule. (To see this, let S be any set of generators of $\mathfrak{m}$, let $\mathfrak{a}$ be the module generated freely by this set, and let $\mathfrak{b}$ be the kernel of the homomorphism obtained by mapping each element of S in $\mathfrak{a}$ to the associated element of $\mathfrak{m}$.)

2 The subject matter

In this chapter, when Dedekind uses the word module, he is referring to a subgroup of $\langle \mathbb{C}, 0, + \rangle$. But any abelian group can be viewed as a $\mathbb{Z}$-module, by interpreting nx as $x + x + \ldots + \ldots x$ (n times) whenever n is a positive integer and x is an element of the group. Dedekind is primarily interested in finitely generated submodules of the complex numbers, and it turns out that any such module is free.

In short, then, Dedekind is concerned with finitely generated free $\mathbb{Z}$-modules. Here are some examples:

- the integers $\mathbb{Z}$, generated by $\{1\}$
- the Gaussian integers $\mathbb{Z}[i]$, generated by $\{1, i\}$
- the integers divisible by 5, denoted $5\mathbb{Z}$, generated by $\{5\}$
- the Gaussian integers divisible by 2, generated as a $\mathbb{Z}$-module by $\{2, 2i\}$
- the Gaussian integers divisible by $1 + i$, generated as a $\mathbb{Z}$-module by $\{1 + i, 1 - i\}$.

You should check the last claim. (Notice that $(1 + i)i = -(1 - i)$.) The example is a little confusing. By definition, the set of Gaussian integers divisible by $1 + i$ consists of all multiples of $1 + i$ by *Gaussian integers*, whereas as set of generators has to yield all of them as linear combinations of multiples by elements of $\mathbb{Z}$. This idea — ignoring various features of a structure at times — is central to algebraic number theory. For example, $\mathbb{Q}(i)$ is a *field*, but we can also view it as a *vector space* over $\mathbb{Q}$ by "forgetting" complex multiplication. Similarly, the Gaussian integers $\mathbb{Z}[i]$ form a ring in their own right, but can also be construed as a module over the smaller ring $\mathbb{Z}$.

Dedekind derives many fundamental properties of such modules, gathering information about their bases, transformations, and submodules. Most of what he does holds more generally for modules over a principle ideal domain, but we will not need the extra generality. Below, I will use word "module" for "$\mathbb{Z}$-module," following Dedekind's use.

Note, incidentally, that in the text the first statement of a numbered subsection is often the statement of a theorem, which the rest of the subsection is devoted to proving.

3 The main definitions and theorems

Let us write, with Dedekind, $[\alpha_1, \ldots, \alpha_k]$ for the submodule of the complex numbers generated by α_1 to α_k, i.e. the set of all finite sums

$$\sum_{i=1}^{n} u_i \alpha_i$$

where each u_i is an element of $\mathbb{Z}$. Considering as an example $\mathbb{Z}$ itself as a $\mathbb{Z}$-module, note that if m and n are integers, m divides n if and only if $[m] \supseteq [n]$. (For example, $[3] \supseteq [6]$.) More generally, Dedekind says that a module $\mathfrak{b}$ divides another module $\mathfrak{a}$ if and only if $\mathfrak{b} \supseteq \mathfrak{a}$. This requires getting used to, because the bigger set "divides" the smaller. It might help to think of $\mathfrak{b}$ dividing $\mathfrak{a}$ in terms of $\mathfrak{b}$ being "finer" than $\mathfrak{a}$.

Dedekind's definitions are otherwise straightforward. The least common multiple of two modules (sitting inside a bigger module, in this case, the complex numbers) is their intersection, and the greatest common divisor consists of sums of elements in each. The notion of equivalence modulo a submodule is just the usual algebraic notion. Dedekind uses $(\mathfrak{b}, \mathfrak{a})$ to denote the number of cosets of $\mathfrak{b}$ modulo $\mathfrak{a}$; we would today call this the cardinality of the quotient structure $\mathfrak{b}/\mathfrak{a}$.

(In Dedekind's treatment, $\mathfrak{a}$ does not have to be a submodule of $\mathfrak{b}$ in the expression $(\mathfrak{b}, \mathfrak{a})$. But, as he points out, in that case the result is the same as what one would get by replacing $\mathfrak{a}$ by $\mathfrak{a} \cap \mathfrak{b}$. I, personally, find it confusing to think of quotients by anything other than a substructure, so in the summary below I will often state Dedekind's theorems in the more restrictive terms. Also, keep in mind that the summary below is not exhaustive.)

The central theorem of Section 3 is as follows. Suppose $\mathfrak{a}$ is a submodule of $\mathfrak{b} = [\beta_1, \ldots, \beta_n]$, such that every element of $\mathfrak{b}/\mathfrak{a}$ is of finite order (in other words, for every b in $\mathfrak{b}$, some multiple nb by a rational integer is in $\mathfrak{a}$). Then $(\mathfrak{b}, \mathfrak{a})$ is finite. Moreover, Dedekind shows how to find a set of generators $\alpha_1, \ldots, \alpha_n$ for $\mathfrak{a}$ such that the α's are obtained from the β's in a nice way, i.e. by a lower-triangular matrix. Then $(\mathfrak{b}, \mathfrak{a})$ is just the determinant of this matrix, in this case, the product of the elements along the diagonal. (Dedekind uses μ's instead of α's, since they are elements of $\mathfrak{m} = \mathfrak{a} \cap \mathfrak{b}$, as in the preceeding parenthetical remark; my use of α is more natural in the context of the summary below.)

Note that when Dedekind uses the word "basis," he really means "set of generators," which is to say, he does not require that they be independent. The notion of independence is introduced in Section 4; at the risk of confusion, I will use "basis" in the modern sense to mean "independent set of generators".

There is a lot going on in Section 4. In 4.2, Dedekind shows

Theorem 3.1 *If one applies the transformation defined by an $n \times n$ matrix (c) with rational entries to an independent set $\alpha_1, \ldots, \alpha_n$, the resulting set of numbers $\alpha'_1, \ldots, \alpha'_n$ will be independent if and only if the determinant C of (c) is nonzero.*

Note that here I am following Dedekind's practice of using (c) to denote the matrix, and C to denote its determinant; modern presentations are more likely to use C for the matrix. Combining this with information from the preceeding section, we have the following very important fact: a submodule of a free module is another free module. In other words, if $\mathfrak{b}$ is a module, $\mathfrak{a}$ is a submodule, and $\mathfrak{b}$ has a basis, then $\mathfrak{a}$ has a basis too.

In 4.3, Dedekind shows the following:

Theorem 3.2 *Let $\alpha_1, \ldots, \alpha_n$ be a basis for a module $\mathfrak{a}$, and let $\alpha'_1, \ldots, \alpha'_n$ be elements of $\mathfrak{a}$. Then $\alpha'_1, \ldots, \alpha'_n$ is a basis for $\mathfrak{a}$ if and only if there is a unimodular matrix (e) (that is, a matrix with determinant ± 1) with entries in $\mathbb{Z}$ transforming one into the other.*

We have already discussed the proof of this in class: if there is such a matrix, it has an inverse transforming the second set back into the first; conversely, if there are matrices transforming each set into the other, their product has to be the identity, which has determinant 1. A similar argument shows that any two bases have to have the same number of elements. (This is a nice property of free $\mathbb{Z}$-modules, and modules over a principle ideal domain more generally.)

In 4.4, Dedekind shows the following:

Theorem 3.3 *If a matrix* (b) *whose entries are (rational) integers transforms a basis* $\beta_1, \ldots, \beta_n$ *of a module* $\mathfrak{b}$ *into a basis* $\alpha_1, \ldots, \alpha_n$ *of a submodule* $\mathfrak{a}$*, then* $(\mathfrak{b}, \mathfrak{a})$ *is the determinant of* (b)*.*

The property of the lower-diagonal matrix described in section 3 is just a particular instance of this.

In 4.5, Dedekind shows the following:

Theorem 3.4 *Suppose* $\mathfrak{a}$ *is generated by* $\alpha_1, \ldots, \alpha_m$*. Suppose that some subset of* n *of them are independent, but there is no independent subset with more than* n *elements. Then there is a basis of* n *elements,* $\alpha'_1, \ldots, \alpha'_n$*.*

This is subtle: it is not necessarily the case that n of the α's can serve as a basis, but Dedekind is thorough in explaining how one can find suitable α''s. In fact, he is computationally explicit. Suppose the α's are given in terms of linear combinations of a basis for a larger module, $\omega_1, \ldots, \omega_n$ by a matrix (r). Dedekind shows how to find the α''s in terms of $\omega_1, \ldots, \omega_n$ by a matrix (e), and then express the original α's in terms of the α's by a matrix (p).

He then works through an example. Let $\mathfrak{a}$ denote the module generated by the following four numbers, described relative to a basis ω_1, ω_2 of a bigger module $\mathfrak{b}$ (i.e. a module dividing $\mathfrak{a}$):

$$\begin{aligned}\alpha_1 &= 21\omega_1 \\ \alpha_2 &= 7\omega_1 + 7\omega_2 \\ \alpha_3 &= 9\omega_1 - 3\omega_2 \\ \alpha_4 &= 8\omega_1 + 2\omega_2\end{aligned}$$

For concreteness, you can think of $\mathfrak{a}$ as being the submodule of $\mathbb{Z}[i]$ generated by $\alpha_1, \ldots, \alpha_4$, with $\omega_1 = 1, \omega_2 = i$.

The preceeding considerations tell us that we should be able to find a basis of $\mathfrak{a}$ with *two* elements, α'_1, α'_2; and that we should be able to represent α'_1 and α'_2 in terms of ω_1, ω_2 by a lower-triangular matrix. Dedekind carries out the calculation to find

$$\begin{aligned}\alpha'_1 &= 21\omega_1 \\ \alpha'_2 &= -17\omega_1 + \omega_2.\end{aligned}$$

With this representation, it is easy to see that $(\mathfrak{b}, \mathfrak{a}) = 21 \times 1 = 21$. Furthermore, Dedekind finds the matrices that express the α's in terms of the α''s and vice versa.

4 Additional notes

There are useful ways of thinking of finitely generated free $\mathbb{Z}$-modules and their submodules in terms of lattices and sublattices. Matrices transform lattices; the number of elements in a quotient corresponds to the number of elements of the finer lattice in a fundamental region of the larger one. I will supply a short excerpt from Jay Goldman's *The Queen of Mathematics: a historically motivated guide to number theory* that discusses this perspective.

Recall that Dedekind shows that if $\mathfrak{b}$ is a free module with basis $\beta_1, \ldots, \beta_n$ and $\mathfrak{a}$ is a submodule of $\mathfrak{b}$ such that $\mathfrak{b}/\mathfrak{a}$ is finite, then $\mathfrak{a}$ is also free, and $\mathfrak{a}$ has a basis of n elements obtained from the β's by a lower diagonal matrix. This makes it easy to read off the cardinality of $\mathfrak{b}/\mathfrak{a}$. If we are allowed to use a *different* basis of $\mathfrak{b}$, we can do even better: there are a basis $\beta'_1, \ldots, \beta'_n$ of $\mathfrak{b}$ and another basis $u_1\beta'_1, \ldots, u_n\beta'_n$ of $\mathfrak{a}$, where $u_1, \ldots, u_n$ are integers, and, moreover, $u_1|u_2|\ldots|u_n$. In other words, the basis of $\mathfrak{a}$ is obtained from the basis of $\mathfrak{b}$ by a very specific type of diagonal matrix. This makes the structure of $\mathfrak{b}/\mathfrak{a}$ very transparent.

Remember that, viewing abelian groups as $\mathbb{Z}$-modules, any finite abelian group can be represented as such a quotient. So the net result is a structure theorem for finite abelian groups. If $\mathfrak{a}$ is presented via a set of generators given in terms of a basis of $\mathfrak{b}$, then describing a group as $\mathfrak{b}/\mathfrak{a}$ in this way is known as "defining a group by generators and relations." The results just described generalize to modules over a principle ideal domain, and to submodules $\mathfrak{a}$ of $\mathfrak{b}$ that have smaller rank (that is, a smaller basis, in which case $\mathfrak{b}/\mathfrak{a}$ is no longer finite). A modern presentation of the relevant structure theorem, specialized to abelian groups, is found in the excerpt from Stewart and Tall's *Algebraic Number Theory and Fermat's Last Theorem.* The same proof is found in Hungerford's *Algebra*, but a later appendix also sketches a more explicitly algorithmic proof, which shows how to actually find the relevant bases for $\mathfrak{b}$ and $\mathfrak{a}$. So, these two presentations yield another opportunity for contrasting "structural" and "algorithmic" proofs of the same theorem.