SUPPLEMENT TO CHAPTER VI

Principal ideal domains

This chapter investigates finitely generated modules over prinvipal ideal domains. Recall that an integral domain R is called an principal ideal domain or PID, if every ideal $I \subseteq R$ is generated by one element, that is, there is an $h \in R$ so that

$$I = (h) = \{ah \,|\, a \in R\}.$$

From MTH310 we know that the ring of integers $\mathbb{Z}$ and the polynomial ring $F[x]$ in one variable over a field F are principal ideal domains. In this class we are mostly interested in modules over $F[x]$, where F is a field. Therefore we may assume in the following that R is either the ring of integers $\mathbb{Z}$ or the polynomial ring $F[x]$ in one variable over a field.

Note. In MTH310 you have seen other examples for principal ideal domains. For example, the rings

$$\mathbb{Z}[i] = \{a + bi \,|\, a, b \in \mathbb{Z}\}, \quad \text{the ring of Gaussian numbers}$$

or

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Z}\}$$

are other examples of principal ideal domains. However, the rings

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \,|\, a, b \in \mathbb{Z}\}$$

and

$$\mathbb{Z}[x] \quad \text{or} \quad F[x, y]$$

are examples of rings which fail to be principal ideal domains.

Properties of principal ideal domains:
(a) Every PID R (if R is not a field) contains prime elements. A nonzero element $p \in R$ is called a *prime element* if p is not a unit in R and has the following property:

$$\text{whenever} \quad a, b \in R \quad \text{with} \quad p \,|\, ab \quad \text{then} \quad p \,|\, a \quad \text{or} \quad p \,|\, b.$$

The prime elements of $\mathbb{Z}$ are the prime numbers and the prime elements of $F[x]$ are called irreducible polynomials. In the following we will refer to the prime elements of R.
(b) Every nonzero, non unit $a \in R$ can be written as a product:

$$a = p_1 p_2 \dots p_n$$

where $p_i \in R$ are prime elements. This decomposition of a into a product of prime elements is unique up to order and associates.
(c) Let $a, b \in R - \{0\}$ be two nonzero elements of R. Then a *greatest common divisor* d of a and b exists, that is, d is a common divisor of a and b and if c is another common divisor of a and b then $c \,|\, d$. Moreover, there are elements $u, v \in R$ so that

$$d = ua + vb.$$

(d) Let $a, b \in R - \{0\}$ be two nonzero elements of R. Then a *least common multiple* m of a and b exists, that is, m is a common multiple of a and b and if ℓ is another common multiple of a and b then $m \,|\, \ell$. If d is a greatest common divisor of a and b and m a least common multiple then

$$ab = u(md)$$

where $u \in R^*$ is a unit.

Cyclic modules

As before assume that R denotes the ring of integers $\mathbb{Z}$ or the polynomial ring $F[x]$ where F is a field.

Definition. An R-module M is called cyclic if M is generated by one element, that is, there is an $m \in M$ so that $M = \{am \,|\, a \in R\}$.

Cyclic modules are the considered the simplest possible R-modules. They are always isomorphic to the R-module R/I where I is an ideal of R:

Proposition A. *Let M be a cyclic R-module. Then there is an ideal $I \subseteq R$ so that the R-modules M and R/I are isomorphic. Moreover, $I = ann(M)$.*

Proof. Assume that $M = \{am \,|\, a \in R\}$ where $m \in M$ is the generator of M. Let $I = \operatorname{ann}(M)$ and define a map:

$$\varphi : R/I \longrightarrow M$$

by $\varphi(a + I) = am$. Since $bm = 0$ for all $b \in I$, the map φ is well defined. It is easy to see that φ is an R-linear map.

Moreover, if R/I and M are isomorphic as R-modules, R/I and M must have the same annihilator. Since the annihilator of R/I is I, we must have that $\operatorname{ann}(M) = I$.

Proposition B. *Let M be a cyclic R-module and N an R-module. Then*

(a) *If $\nu : M \longrightarrow N$ is a surjective R-linear map, then N is cyclic.*
(b) *Every submodule of M is cyclic.*

Proof. (b) Suppose that M is generated by $m \in M$, that is,

$$M = \{am \,|\, a \in R\}.$$

For a submodule $T \subseteq M$ consider the following subset of R:

$$I = \{a \in R \,|\, am \in T\}.$$

It is easy to check that I is an ideal of R. Since R is $\mathbb{Z}$ or $F[x]$ every ideal of R is principal, that is, there is an element $b \in I$ so that $I = \{ab \,|\, a \in R\}$, we have $T = \{a(bm) \,|\, a \in R\}$ and T is cyclic, generated by bm.

It can happen that direct sums of cyclic modules are cyclic again. For example,

$$\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6.$$

In general, we have:

Theorem C. *Let $I = (a)$ and $J = (b)$ be ideals of R. Then*

$$R/I \times R/J$$

is a cyclic module if and only if a and b are relatively prime. In this case,

$$R/I \times R/J \cong R/K$$

where $K = (ab)$.

Proof. Suppose that $R/I \times R/J$ is a cyclic R-module and let $(n + (a), m + (b))$ be a generator of $R/I \times R/J$. Then there is an element $s \in R$ so that

$$s(n + (a), m + (b)) = (sn + (a), sm + (b)) = (1 + (a), 0 + (b)).$$

Thus for some $u \in R$, $sn = 1 + ua$. This shows that n and a are relatively prime. Similarly, there is an element $t \in R$ so that

$$t(n + (a), m + (b)) = (tn + (a), tm + (b)) = (0 + (a), 1 + (b))$$

and m and b are relatively prime. Moreover, $sm + (b) = 0 + (b)$ implies that $b \mid sm$ and thus $b \mid s$ since m and b are relatively prime. Substitute $s = cb$ into the equation $sn = 1 + ua$. Then $1 = ua + (-cn)b$. a and b are relatively prime.

Conversely, suppose that a and b are relatively prime. Then there are elements $u, v \in R$ so that

$$ua + vb = 1.$$

Define

$$\varphi : R/(ab) \longrightarrow R/(a) \times R/(b)$$

by $\varphi(x + (ab)) = (x + (a), x + (b))$. It is easy to show that φ is a well defined R-linear map. We need to show that φ is injective and surjective. If $\varphi(x + (ab)) = (0 + (a), 0 + (b))$ then $a \mid x$ and $b \mid x$ and thus $ab \mid x$ since a and b are relatively prime. Therefore $x + (ab) = 0 + (ab)$ and φ is injective.

In order to show that φ is surjective, let $(m + (a), n + (b)) \in R/(a) \times R/(b)$. Then $\varphi(una + vmb + (ab)) = (vmb + (a), una + (b))$. Since $m \equiv vmb \bmod a$ and $n \equiv una \bmod b$ we have that $\varphi(una + vmb + (ab)) = (m + (a), n + (b))$ and φ is surjective.

The primary decomposition theorem

In the following let M be a finitely generated module over R, where R is a PID. We also assume that M has a nonzero annihilator, that is, $\operatorname{ann}(M) = I \neq (0)$.

Theorem D.

$$M \cong R/(p_1^{e_1}) \times R/(p_2^{e_2}) \times \ldots \times R/(p_r^{e_r})$$

where $p_i \in R$ are prime elements. Moreover, this decomposition of M is unique in the following sense. If

$$M \cong R/(q_1^{f_1}) \times R/(q_2^{f_2}) \times \ldots \times R/(q_s^{f_s})$$

then $r = s$ and, after renumbering (if necessary), $p_i^{e_i}$ and $q_i^{f_i}$ are associates.

Note that the prime elements p_i in Theorem are not necessarily distinct, that is, possibly $p_i = p_j$ or p_i associated to p_j if $i \neq j$.

Definition. The ideals $(p_1^{e_1}), \ldots, (p_r^{e_r})$ are called the *elementary divisors* of M.

Remark. Theorem D states that the R-module M can be written as

$$M = N_1 \oplus N_1 \oplus \ldots \oplus N_r$$

where N_i are cyclic submodules of M with $N_i \cong R/(p_i^{e_i})$ for all $1 \leq i \leq r$.

Corollary E. *Let M, N be finitely generated R-modules with $ann(M) \neq (0)$ and $ann(N) \neq (0)$. M and N are isomorphic if and only if M and N have the same elementary divisors.*

Corollary F. *Suppose that M decomposes as in Theorem D:*

$$M \cong R/(p_1^{e_1}) \times R/(p_2^{e_2}) \times \ldots \times R/(p_r^{e_r}).$$

Then $ann(M) = (d)$ where d is the least commmon multiple of $p_1^{e_1}, \ldots, p_r^{e_r}$.

The invariant factor decomposition

Again, assume that R is a PID and every R-module M is finitely generated with nontrivial annihilator, that is, $\text{ann}(M) \neq (0)$.

Theorem G.

$$M \cong R/(d_1) \times R/(d_2) \times \ldots \times R/(d_m)$$

where

$$d_m \,|\, d_{m-1} \,|\, \ldots \,|\, d_2 \,|\, d_1.$$

The scalars d_i are called the invariant factors of M. The invariant factors of M are uniquely determined by the module M (up to multiplication by a unit).

Definition. The ideals $(d_1), (d_2), \ldots, (d_m)$ are called the *invariant factor ideals* of M.

Remark. Theorem G states that the R-module M can be written as

$$M = N_1 \oplus N_1 \oplus \ldots \oplus N_m$$

where N_i are cyclic submodules of M with $N_i \cong R/(d_i)$ for all $1 \leq i \leq m$. Moreover,

$$(d_1) \subseteq (d_2) \subseteq \ldots \subseteq (d_m)$$

Corollary H. *Let M, N be finitely generated R-modules with $ann(M) \neq (0)$ and $ann(N) \neq (0)$. M and N are isomorphic if and only if M and N have the same invariant factor ideals.*

Corollary I. *Suppose that M decomposes as in Theorem G:*

$$M \cong R/(d_1) \times R/(d_2) \times \ldots \times R/(d_m)$$

where

$$d_m \,|\, d_{m-1} \,|\, \ldots \,|\, d_2 \,|\, d_1.$$

Then $ann(M) = (d_1)$.

In the following chapter we will investigate how to make use of Theorems D and G in order to answer our main questions on similar operators and matrices:

(1) Let $\sigma, \tau \in \mathcal{L}(V)$. How do we decide if σ and τ are similar? We have already seen that σ and τ are similar if and only if V_σ and V_τ are isomorphic as $F[x]$-modules. By Theorem D this is equivalent to V_σ and V_τ having the same elementary divisors (up to order and associates). We can also use Theorem G which states that V_σ and V_τ are isomorphic if and only if they have the same invariant factor ideals.

(2) Given two $n \times n$-matrices A and B. How do we decide if A and B are similar?

(3) Let V be a finite dimensional vector space and $\tau \in \mathcal{L}(V)$. An obvious question which arises from (1) is how to find the elementary divisors and invariant factors of V_τ?