Algebraic Number Theory

Lecture 4, 29th October 2021

1.3 Modules

Definition 1.33 Let R be a commutative unitary ring.

A <u>R-module</u> consists of an abelian group $(M,+)$ and a scalar multiplication

$$R \times M \longrightarrow M$$
$$(\alpha, x) \longmapsto \alpha x$$

such that for all $x, y \in M$ and $\alpha, \beta \in R$ we have

i) $(\alpha\beta)x = \alpha(\beta x)$

ii) $(\alpha+\beta)x = \alpha x + \beta x$
$\alpha(x+y) = \alpha x + \alpha y$

iii) $1 \cdot x = x$

Remark 1.34

i) If R is a field R-modules are R-vector spaces

ii) We can define R-modul homomorphism, submodules, quotient modules similar as linear maps, subspaces and quotient spaces.

iii) Every R is a R-module over itself. its submodules are exactly the ideals of R.

Definition 1.35 i) Let $A \subseteq M$ be a subset of an R-module M. Then $\langle \emptyset \rangle := \{0\}$

$$\langle A \rangle = \left\{ \sum_{i=1}^{n} r_i a_i \;\middle|\; n \geq 1,\ r_i \in R,\ a_i \in A \right\}$$

denotes the <u>submodule of M generated by A</u>.

ii) If $\langle A \rangle = M$ then A is called a <u>generating set of M.</u> If there exist a finite A with $\langle A \rangle = M$ then M is called <u>finitely generated.</u>

iii) A family $(m_\lambda)_{\lambda \in \Lambda}$ of elements $m_\lambda \in M$ are called <u>linearly independent</u> if

$$\sum_{\lambda \in \Lambda} r_\lambda m_\lambda = 0$$

with $r_\lambda \in R$ ($r_\lambda = 0$ for all but fin. many) implies $r_\lambda = 0$ for all $\lambda \in \Lambda$.

iv) A lin. independendent gen. set is called a <u>basis.</u>

v) If M has a basis then M is called <u>free</u>.

Remark 1.36

(Linear algebra)

i) If R is a field then every R-module is free.

ii) The $\mathbb{Z}$-module $M = \mathbb{Z}/2\mathbb{Z}$ $(r \cdot \bar{m} = \overline{r \cdot m})$ is not free.

$A = \{\bar{0}\}$ does not generate M

$A = \{\bar{1}\}, \{\bar{0}, \bar{1}\}$ are not lin. independent, since $2 \cdot \bar{1} = \bar{0}$

Proposition 1.37 Let R be a com. unitary ring. For a R-module the following two statements are equivalent:

i) Every submodule of M is finitely generated.

ii) Any sequence $M_1 \subset M_2 \subset \dots$ of submodules of M eventually stabilizes, i.e. for some n we have $M_n = M_{n+1} = M_{n+2} = \dots$.

Proof: HW2

Definition 1.38 i) A R-module which satisfies one of the conditions in Prop. 1.37 is called a <u>noetherian module</u> (named after Emmy Noether)

ii) A ring is called <u>noetherian</u> if it is a noetherian module over itself.

Examples 1.39 i) Fields are noetherian.

ii) The following ring is not noetherian:

$$R = \{ f(x) \in \mathbb{Q}[x] \mid f(0) \in \mathbb{Z} \}$$
$$\overset{!}{=} \{ f = m + Xg \mid m \in \mathbb{Z}, g \in \mathbb{Q}[X] \}$$

Now define for $n \geq 1$ the ideals/submodules

$$M_n := \left\{ aX + h(x) \;\middle|\; a = \frac{m}{2^n},\ \begin{array}{l} m \in \mathbb{Z} \\ h(x) \in X\mathbb{Q}[X] \end{array} \right\}.$$

we get a sequence of ideals/submodules

$$M_1 \subset M_2 \subset \dots$$

which does not stabilizes.

iv) The ring $R = \mathbb{Q}[x_1, x_2, \ldots]$ is fin. gen as a R-module. But it is not noetherian since the ideal $\langle x_1, x_2, \ldots \rangle$ is not fin. gen.

Proposition 1.40 Let R be a noetherian ring and M a R-module. Then M is noetherian if and only if M is finitely generated.

Proof: HW2

Corollary 1.41

i) PIDs are noetherian

ii) Finitely gen. modules over PIDs are noetherian.

Proof: i) Principal ideals are fin. generated.

ii) follows from Prop 1.40. $\square$

§ 2 Integrality

Definition 2.1

i) An <u>algebraic number field</u> (ANF) K is a finite field extension of $\mathbb{Q}$.
(i.e. $\mathbb{Q} \subset K$ and $\dim_{\mathbb{Q}} K < \infty$)

The elements of K are called <u>algebraic numbers</u>.

ii) A number $x \in K$ of a ANF is called an <u>algebraic integer</u> if it is the zero of a monic polynomial with integer coefficients, i.e

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0$$

for some $a_1, \ldots, a_n \in \mathbb{Z}$.

We set

$$\mathcal{O}_K = \{ x \in K \mid x \text{ alg. integer} \}.$$

This is called the <u>ring of integers</u> of K.

From the definition it is not clear that $\mathcal{O}_K$ is actually a ring. To see this we will study the notion of integrality in general.

<u>Definition 2.2</u> Let $A \subseteq B$ be an extension of rings. An element $b \in B$ is called <u>integral over A</u>, if it satisfies a monic equation

$$X^n + a_1 X^{n-1} + \dots + a_n = 0 \quad , \quad n \geq 1$$

with coefficients $a_i \in A$. The ring B is called integral over A if all elements $b \in B$ are integral over A.

We want to show that sums and products of integral elements are again integral.

<u>Proposition 2.3</u> Elements $b_1, \dots, b_n \in B$ are all integral over A if and only if $A[b_1, \dots, b_n]$ is finitely generated as a A-module.

To prove this we recall the following fact from linear algebra.

(Laplace expansion)

Proposition 2.4 Let $A = (a_{ij})$ be an $(r \times r)$-matrix with entries in a ring R, and let $A^* = (a^*_{ij})$ be the adjoint matrix, i.e.

$$a^*_{ij} = (-1)^{i+j} \det(A_{ij}),$$

where A_{ij} is obtained from A by deleting the i-th column and j-th row.

$$A_{ij} = \begin{array}{c} i \\ \left(\begin{array}{c|c} & \\ \hline & \end{array} \right) j \\ A \end{array}$$

Then

$$AA^* = A^*A = \det(A)\,E. \qquad (E \text{ unit matrix})$$

In particular, for $x \in R^r$ we get

$$Ax = 0 \implies \det(A) \cdot x = 0$$

Proof: See linear algebra and notice that it works for rings and not just fields. $\square$

Proof of Proposition 2.3: "$\Rightarrow$":

- Let b be integral over A, i.e $f(b)=0$ for some monic polynomial $f(x) \in A[x]$ of degree $m \geq 1$.

  Since f is monic we can write any $g(x) \in A[x]$ as

$$g(x) = q(x) f(x) + r(x)$$

for some $q(x), r(x) \in A[x]$ with $\deg(r) < m$.

Therefore

$$g(b) = r(b) = a_0 + a_1 b + \dots + a_{m-1} b^{m-1}$$

with $a_i \in A$.

$\Rightarrow$ $A[b]$ is generated by $1, b, \dots, b^{m-1}$.

If $b_1, \dots, b_n$ are integral over A we see by induction on n that $A[b_1, \dots, b_n]$ is finitely generated.

"$\Leftarrow$"

- Conversely assume that $A[b_1,\dots,b_n]$ is fin. gen. by $\omega_1,\dots,\omega_r$. Then for any $b \in A[b_1,\dots,b_n]$ we can write

$$b\omega_i = \sum_{j=1}^{r} a_{ij}\,\omega_j \qquad a_{ij} \in A.$$

$$\left(\underbrace{\begin{pmatrix} & & \\ & a_{ij} & \\ & & \end{pmatrix}}_{S} \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_r \end{pmatrix} = \begin{pmatrix} b\omega_1 \\ b\omega_2 \\ \vdots \\ b\omega_r \end{pmatrix} \right) \qquad S = (a_{ij})$$

By Proposition 2.4 we get

$$\underbrace{\det(bE - S)\,\omega_i}_{f_i} = 0 \quad . \quad (\star)$$

for all $i = 1,\dots,r$.

Moreover since $1 \in A[b_1,\dots,b_n]$ we can write

$$1 = c_1\omega_1 + \dots + c_r\omega_r \quad \text{with } c_i \in A.$$

$$\overset{(\star)}{\Longrightarrow} \quad \sum_{i=1}^{r} c_i f_i = \det(bE - S) = 0.$$

Since

$$\det(bE - S) = b^r + a_1 b^{r-1} + \dots + a_r \qquad a_i \in A$$

we obtain that b is integral over A.

$\square$

Corollary 2.5 If b_1 and b_2 are integral over A, then $b_1 + b_2$ and $b_1 \cdot b_2$ are also integral over A.

Definition 2.6 Let $A \subseteq B$ be a ring extension,

i) The ring $\overline{A} = \{ b \in B \mid b \text{ integral over } A \}$ is called the <u>integral closure of A in B</u>.

ii) If $\overline{A} = A$ then A is called <u>integrally closed</u> in B.

In particular: If K is an ANF, then $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K.

$\mathcal{O}_K = \overline{\mathbb{Z}}$

Proposition 2.7. Let $A \subseteq B \subseteq C$ be two ring extensions. If B is integral over A and C is integral over B, then C is integral over A.