

## LECTURE 10: INTEGRAL EXTENSIONS

GIRJA SHANKER TRIPATHI

In all the discussions that follow  $A$  is a commutative ring with identity.

### 1. DEFINITIONS

**Definition 1.1.** An  $A$ -module  $M$  is said to be finitely generated, if there exist elements  $m_1, \dots, m_n \in M$  such that every element of  $M$  is an  $A$ -linear combination of  $m_1, \dots, m_n$ .

In other words, for a given  $m \in M$ , there are ring elements  $a_1, \dots, a_n$  such that  $m = a_1m_1 + \dots + a_nm_n$ . This is equivalent to the fact that the ring homomorphism  $\varphi : \bigoplus_{i=1}^n Ae_i \longrightarrow M$  defined by  $\sum a_i e_i \mapsto \sum a_i m_i$  is surjective.

**Definition 1.2.** An  $A$ -algebra  $B$  is said to be finitely generated if there exist elements  $b_1, \dots, b_n$  in  $B$  such that the evaluation homomorphism  $\phi : A[x_1, \dots, x_n] \longrightarrow B$  defined by  $f(x_1, \dots, x_n) \mapsto f(b_1, \dots, b_n)$  is surjective, where  $P[x_1, \dots, x_n]$  is the polynomial ring in  $n$ -variables over  $A$  and  $f(x_1, \dots, x_n)$  is a polynomial in  $P[x_1, \dots, x_n]$ .

This means that, for a given  $b \in B$ , there exists a polynomial  $f(x_1, \dots, x_n) \in P[x_1, \dots, x_n]$  such that  $b = f(b_1, \dots, b_n)$ .

**Definition 1.3.** A field  $K$  is said to be finitely generated over its subfield  $k$ , if there exist elements  $c_1, \dots, c_n$  in  $K$  such that every element of  $K$  is a rational function of  $c_1, \dots, c_n$ .

That is, for a given  $\alpha$  in  $K$ , there exist polynomials  $f(x_1, \dots, x_n), g(x_1, \dots, x_n) \in k[x_1, \dots, x_n]$  such that  $\alpha = f(c_1, \dots, c_n)/g(c_1, \dots, c_n)$ , where  $g(c_1, \dots, c_n) \neq 0$ . In this case, we write that  $K = k(c_1, \dots, c_n)$ .

**Definition 1.4.** If an  $A$ -algebra  $B$  is finitely generated as an  $A$ -module, we say that  $B$  is finite over  $A$ .

Clearly, if  $B$  is finite over  $A$ , then  $B$  is finitely generated over  $A$ . But the converse need not be true. For example, consider the polynomial ring  $A[x] = A \oplus Ax \oplus Ax^2 \dots$ , in one variable  $x$  over  $A$ . This is clearly a finitely generated  $A$ -algebra, but it is not finitely generated  $A$ -module.

**Definition 1.5.** Let  $B$  be an  $A$ -algebra. An element  $b$  of  $B$  is said to be integral over  $A$ , if there exists a monic polynomial  $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$  in  $A[x]$  such that  $f(b) = b^n + a_{n-1}b^{n-1} + \dots + a_1b + a_0 = 0$ .

**Proposition 1.6.** Let  $A$  be a subring of  $B$  and  $b \in B$ . Then the following are equivalent:

1.  $b$  is integral over  $A$ ;
2.  $A[b]$  is finite  $A$ -algebra; and

---

*Date:* November 1, 2005.

3. *There exists a finite  $A$ -algebra  $C$ , such that  $A \subset C \subset B$  and  $b \in C$*

*Proof.* We first prove that (1) implies (2). Since  $b$  is integral over  $A$ , we have  $b^n + a_1b^{n-1} + \dots + a_{n-1}b + a_n = 0$ , where  $a_1, \dots, a_n$  are elements of  $A$ . This equation gives us that  $b^n = -(a_1b^{n-1} + \dots + a_{n-1}b + a_n)$ . We assert that every nonnegative integral power of  $b$  can be expressed as an  $A$ -linear combination of  $1, b, \dots, b^{n-1}$ . This is true for  $b^n$  in view of above. Suppose  $b^m$  can be expressed as an  $A$ -linear combination of  $1, b, \dots, b^{n-1}$ . Let  $b^m = c_{n-1}b^{n-1} + \dots + c_1b + c_0$ , where  $c_0, \dots, c_{n-1} \in A$ . Then we have,  $b^{m+1} = b(-(c_{n-1}b^{n-1} + \dots + c_1b + c_0)) = -(c_{n-1}b^n + c_{n-2}b^{n-1} + \dots + c_0b)$ . Expressing  $b^n$  as an  $A$ -linear combination of  $1, b, \dots, b^{n-1}$ , we see that assertion follows from induction. But this means that any  $f \in A[b]$  is an  $A$ -linear combination of  $1, b, \dots, b^{n-1}$ . Therefore,  $A[b]$  is finite  $A$ -algebra.

Clearly (2) implies (3) is trivial (take  $C = A[b]$ ).

We finally prove that (3) implies (1). Suppose  $C = A + Ac_1 + \dots + Ac_n$ , where  $c_i$ 's are elements of  $C$ . Consider  $bc_i = \sum_{j=1}^n a_{ij}c_j$ , where  $a_{ij} \in A$ ;  $i, j = 1, \dots, n$ . This gives  $\sum_{j=1}^n (\delta_{ij}b - a_{ij})c_j = 0$ , where  $\delta_{ij}$  is the Kronecker delta symbol. Consider the matrix  $M = (\delta_{ij}b - a_{ij})$ . For  $c = (c_1, \dots, c_n)^t$ , we have  $Mc = 0$ . Then by Cramer's rule we have  $\det(M)c_i = 0$ , for all  $i$ . This gives that  $\det(M) = 0$ . But  $\det(M)$  is a monic polynomial of degree  $n$  in  $b$ . This proves that  $b$  is integral over  $A$ .  $\square$

**Corollary 1.7.** *Suppose  $A$  be a subring of  $B$ .*

1. *If  $b_1$  and  $b_2$  are integral over  $A$ , then so are  $b_1 + b_2$  and  $b_1b_2$ ;*
2. *The set of elements  $A$  which are integral over  $A$ , is a ring (called the integral closure of  $A$ ); and*
3. *Integrability is transitive; that is, if  $A \in B \in C$  is a tower of rings such that  $C$  is integral over  $B$  and  $B$  is integral over  $A$ , then  $C$  is integral over  $A$ .*

*Proof.* 1. Since  $b_1, b_2$  are integral over  $A$ , we have, for some natural numbers  $m, n$

$$\begin{aligned} A[b_1] &= A + Ab_1 + \dots + Ab_1^m \\ A[b_2] &= A + Ab_2 + \dots + Ab_2^n \end{aligned}$$

Now consider the algebra  $A[b_1, b_2]$ . We have  $A \subset A[b_1, b_2] \subset B$ ; and  $A[b_1, b_2]$  is finitely generated as an  $A$ -module, for the elements  $1, b_1^i b_2^j, i = 1, \dots, m; j = 1, \dots, n$  generate  $A[b_1, b_2]$  over  $A$ . Since  $b_1 + b_2$  and  $b_1b_2$  are in the algebra  $A[b_1, b_2]$ , result follows from above proposition.

2. Follows from part (1) of this corollary.

3. Suppose  $c \in C$ . Since  $C$  is integral over  $B$ , we have for some ring elements  $s_1, \dots, s_n \in B$ ;  $c^n + s_1c^{n-1} + \dots + s_{n-1}c + s_n = 0$ . Consider the ring  $A[s_1, \dots, s_n]$ .  $c$  is integral over  $A[s_1, \dots, s_n]$ , hence  $A[s_1, \dots, s_n][c]$  is finite  $A[s_1, \dots, s_n]$ -module. But  $A[s_1, \dots, s_n]$  is finite  $A$ -module, since  $s_1, \dots, s_n$  are finitely many integral elements over  $A$ . This gives that  $A[s_1, \dots, s_n][c]$  is finite  $A$ -module. Then the result follows from above proposition.  $\square$

- Definition 1.8.**
1. Suppose  $A \subset B$  be a subring of  $B$ . If the ring  $\tilde{A}$  of elements of  $B$ , which are integral over  $A$ , equals  $A$ , we say that  $A$  is integrally closed over  $B$ .
  2. If an integral domain  $A$  is integrally closed over its field of fractions, we say that  $A$  is integrally closed.

**Example 1.9.** An unique factorization domain (UFD) is integrally closed: Suppose that  $A$  be an UFD and  $Q$  be it's field of fractions. Let  $c \in Q$  be integral over  $A$ . Then we have  $c^n + a_1c^{n-1} + \dots + a_{n-1}c + a_n = 0$ , for some  $a_1, \dots, a_n \in A$ . Writing  $c = p/q$ , where  $(p, q) = 1$ , and multiplying above equation by  $q^n$ , we see that  $p^n = -(a_1p^{n-1}q + \dots + a_{n-1}pq^{n-1} + a_nq^n) = -(a_1p^{n-1} + \dots + a_{n-1}pq^{n-2} + a_nq^{n-1})q$ . Since  $(p, q) = 1$ , and  $A$  is UFD, this is not possible unless  $q$  is unit in  $A$ , but then  $c \in A$ . Therefore,  $\tilde{A} = A$ . This proves that  $A$  is integrally closed.

**Example 1.10.** Suppose that  $K \subset \mathbb{Q}$  be a finite algebraic extension of the field  $\mathbb{Q}$  of rational numbers. The subring of algebraic elements of  $K$  over  $\mathbb{Q}$ , is denoted by  $O_K$ , and is called the ring of algebraic integers in  $K$ .

#### REFERENCES

- [1] C. Musili, *Algebraic Geometry for Beginners*, Texts and Readings in Mathematics, Hindustan Book Agency, 2001.

LOUISIANA STATE UNIVERSITY, DEPARTMENT OF MATHEMATICS, BATON ROUGE, LA 70803, USA

*E-mail address:* girja@math.lsu.edu