D Integrality and Algebraic Integers

We recall/introduce here some notions of the *Commutative Algebra* lecture on integrality of ring elements. However, we are essentially interested in the field of complex numbers and its subring $\mathbb{Z}$.

Definition D.1 (*integral element, algebraic integer*)

Let A be a subring of a commutative ring B.

(a) An element $b \in B$ is said to be **integral** over A if b is a root of monic polynomial $f \in A[X]$, that is $f(b) = 0$ and f is a polynomial of the form $X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ with $a_{n-1}, \ldots, a_0 \in A$. If all the elements of B are integral over A, then we say that B is **integral** over A.

(b) If $A = \mathbb{Z}$ and $B = \mathbb{C}$, an element $b \in \mathbb{C}$ integral over $\mathbb{Z}$ is called an **algebraic integer**.

Theorem D.2

Let $A \subseteq B$ be a subring of a commutative ring and let $b \in B$. TFAE:

(a) b is integral over A;

(b) the ring $A[b]$ is finitely generated as an A-module;

(c) there exists a subring S of B containing A and b which is finitely generated as an A-module.

Recall that $A[b]$ denotes the subring of B generated by A and b.

Proof:

(a)$\Rightarrow$(b): Let $a_0, \ldots, a_{n-1} \in A$ such that $b^n + a_{n-1}b^{n-1} + \ldots + a_1b + a_0 = 0$ $(*)$. We prove that $A[b]$ is generated as an A-module by $1, b, \ldots, b^{n-1}$, i.e. $A[b] = A + Ab + \ldots + Ab^{n-1}$. Therefore it suffices to prove that $b^k \in A + Ab + \ldots + Ab^{n-1} =: C$ for every $k \geqslant n$. We proceed by induction on k:

- If $k = n$, then $(*)$ yields $b^n = -a_{n-1}b^{n-1} - \ldots - a_1b - a_0 \in C$.
- If $k > n$, then we may assume that $b^n, \ldots, b^{k-1} \in C$ by the induction hypothesis. Hence multiplying $(*)$ by b^{k-n} yields

$$b^k = -a_{n-1}b^{k-1} - \ldots - a_1b^{k-n+1} - a_0b^{k-n} \in C$$

because $a_{n-1}, \ldots, a_0, b^{k-1}, \ldots, b^{k-n} \in C$.

(b)$\Rightarrow$(c): Set $S := A[b]$.

(c)$\Rightarrow$(a): By assumption $A[b] \subseteq S = Ax_1 + \ldots + Ax_n$, where $x_1, \ldots, x_n \in B$, $n \in \mathbb{Z}_{>0}$. Thus for each $1 \leqslant i \leqslant n$ we have $bx_i = \sum_{j=1}^{n} a_{ij}x_j$ for certain $a_{ij} \in A$. Set $x := (x_1, \ldots, x_n)^{\mathrm{Tr}}$ and consider the $n \times n$-matrix $M := bI_n - (a_{ij})_{ij} \in M_n(S)$. Hence

$$Mx = 0 \qquad \Rightarrow \quad \mathrm{adj}(M)Mx = 0\,,$$

where $\mathrm{adj}(M)$ is the adjugate matrix of M (i.e. the transpose of its cofactor matrix). By the properties of the determinant (GDM), we have

$$\mathrm{adj}(M)M = \det(M)I_n\,,$$

Hence $\det(M)x_i = 0$ for each $1 \leqslant i \leqslant n$, and so $\det(M)s = 0$ for every $s \in S$. As $1 \in S$ this gives us $\det(M) = 0$. It now follows from the definition of M that b is a root of the monic polynomial $\det(X \cdot I_n - (a_{ij})_{ij}) \in A[X]$, thus integral over A.

■

Corollary D.3

Let $A \subseteq B$ be a subring of a commutative ring. Then $\{b \in B \mid b \text{ integral over } A\}$ is a subring of B.

Proof: We need to prove that if $b, c \in B$ are integral over A, then so are $b + c$ and $b \cdot c$. By Theorem D.2(b) and its proof both $A[b] = A + Ab + \ldots + Ab^{n-1}$ and $A[c] = A + Ac + \ldots + Ac^{m-1}$ for some $n, m \in \mathbb{Z}_{>0}$. Thus $S := A[b, c]$ is finitely generated as an A-module by $\{b^i c^j \mid 0 \leqslant i \leqslant n, 0 \leqslant j \leqslant m\}$. Theorem D.2(c) now yields that $b + c$ and $b \cdot c$ are integral over A because they belong to S. ■

Example 13

All the elements of the ring $\mathbb{Z}[i]$ of Gaussian intergers are integral over $\mathbb{Z}$, hence algebraic integers, since i is a root of $X^2 + 1 \in \mathbb{Z}[X]$.

Lemma D.4

If $b \in \mathbb{Q}$ is integral over $\mathbb{Z}$, then $b \in \mathbb{Z}$.

Proof: We may write $b = \frac{c}{d}$, where c and d are coprime integers and $d \geqslant 1$. By the hypothesis there exist $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ such that

$$\frac{c^n}{d^n} + a_{n-1}\frac{c^{n-1}}{d^{n-1}} + \ldots + a_1\frac{c}{d} + a_0 = 0\,,$$

hence

$$c^n + \underbrace{d a_{n-1} c^{n-1} + \ldots + d^{n-1} a_1 + d^n a_0}_{\text{divisible by } d} = 0\,.$$

Thus $d \mid c^n$. As $\gcd(c, d) = 1$ and $d \geqslant 1$ this is only possible if $d = 1$, and we deduce that $b \in \mathbb{Z}$. ■

Clearly, the aforementionnend lemma can be generalised to integral domains (=Integritätsring) and their field of fractions.