**Math 154 Notes 1**

These are some notes on algebraic integers. Let $\boldsymbol{C}$ denote the complex numbers.

**Definition 1:** An *algebraic integer* is a number $x \in \boldsymbol{C}$ that satisfies an integer monic polynomial. That is

$$x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 = 0; \qquad a_0, ..., a_{n-1} \in \boldsymbol{Z}. \tag{1}$$

For instance, a rational number is an algebraic integer if and only if it is an integer.

**Definition 2:** An abelian group $M \subset \boldsymbol{C}$ is a *finitely generated $\boldsymbol{Z}$-module* if there is a finite list of elements $v_1, ..., v_n \in M$, such that every element of $M$ has the form $a_1 v_1 + ... + a_n v_n$ for some $a_1, ..., a_n \in \boldsymbol{Z}$.

**Definition 3:** Let $\boldsymbol{Z}[x]$ be the set of all finite sums of the form $b_0 + b_1 x + b_2 x^2 ...$ with $b_i \in \boldsymbol{Z}$. In other words $\boldsymbol{Z}[x]$ is the set of all integer polynomials in $x$.

The purpose of these notes is to prove two results about algebraic integers. Here is the first result.

**Theorem 0.1** *The following are equivalent.*

1. *$x$ is an eivenvalue of an integer matrix.*
2. *$x$ is an algebraic integer.*
3. *$\boldsymbol{Z}[x]$ is finitely generated.*
4. *There exists a finitely generated $\boldsymbol{Z}$-module $M$ such that $xM \subset M$.*

**Proof:** Suppose $x$ is the eigenvalue of an integer matrix $A$. Then $x$ is a root of the polynomial $\det(xI - A)$, which is an integer monic polynomial. Hence (1) implies (2).

The set $\boldsymbol{Z}[x]$ is clearly an abelian group. If $x$ satisfies Equation 1, then then $x_n, x_{n+1}, ...$ can be expressed as integer combinations of $1, ..., x^{n-1}$. Hence $\boldsymbol{Z}[x]$ is a finitely generated $\boldsymbol{Z}$-module when $x$ is an algebraic integer. Hence (2) implies (3).

We can take $M = \boldsymbol{Z}[x]$. Clearly $xM \subset M$. Hence (3) implies (4).

Now for the one interesting implication. Suppose that $xM \subset M$ and $M$ is finitely generated. We can find elements $v_1, ..., v_n \in M$ such that every element of $M$ is an integer combination of these. In particular, $xv_j \in M$, so

$$xv_j = A_{j1}v_1 + ... + A_{jn}v_n; \qquad A_{ji} \in \boldsymbol{Z}. \tag{2}$$

Let $A$ be the matrix whose entries are $A_{jk}$ and let $V = (v_1, ..., v_n)$. Equation 2 says $AV = xV$. So, $x$ is an eivenvalue of $A$. Hence (4) implies (1). ♠

Here is the second result.

**Theorem 0.2** *The set of algebraic integers is a ring.*

**Proof:** We just have to prove that the set of algebraic integers is closed under addition and multiplication. Suppose that $x$ and $y$ are both algebraic integers. We define $M = \boldsymbol{Z}[x, y]$, the set of polynomial expressions

$$\sum a_{ij}x^iy^j; \qquad a_{ij} \in \boldsymbol{Z}.$$

Note that $M$ is a finitely generated $\boldsymbol{Z}$-module, because high powers of $x$ and $y$ are integer combinations of lower powers. More precisely, if $x$ satisfies an integer monic polynomial of degree $m$ and $y$ satisfies an integer polynomial of degree $n$ then any element of $M$ is an integer combination of the elements $\{x^iy^j\}$ where $i = 0, ..., m-1$ and $j = 0, ..., n-1$.

Setting $z = x + y$, we clearly have $zM \subset M$. Hence $z$ is an algebriac integer, by Theorem 0.1. The same goes for $z = xy$. ♠