Matrix Theory:
Addition of algebraic integers[*]

A real number α is *algebraic number* if it is a root of a polynomial with integer coefficients. For example, $\sqrt{2}$ and $1+\frac{1}{2}\sqrt{7}$ are algebraic numbers, being roots of x^2-2 and $4x^2-8x-3$, respectively.

A real number α is *algebraic integer* if it is a root of a *monic* polynomial with integer coefficient, i.e., of a polynomial whose leading coefficient is 1. So, for example $\sqrt{2}$ is an algebraic integer, but $1+\frac{1}{2}\sqrt{7}$ is not (why?).

Degree of an algebraic number is the least degree of a polynomial of which it is a root. For example, every rational number is an algebraic number of degree 1, whereas every integer is an algebraic integer of degree 1. Hence, the algebraic numbers and algebraic integers are generalizations of rational numbers and integers respectively.

In this note we show that algebraic integers are closed under addition. We treat the special case of $\sqrt{2}+\sqrt{3}$ first, and give a proof of a general next.

Special case: $\sqrt{2}+\sqrt{3}$

We could find a polynomial of which $\sqrt{2}+\sqrt{3}$ is a root by a brute force computation. That would messy, and we are lazy, so instead we do some linear algebra.

Let $\mathcal{B}=\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$. We shall consider the vector space V over $\mathbb{Q}$ (the field of rational numbers) that is spanned by $\mathcal{B}$. One can check $\mathcal{B}$ is linearly independent over $\mathbb{Q}$, and so $\mathcal{B}$ is a basis for V. Let $T\colon V\to V$ be the linear transformation given by

$$T(x)=(\sqrt{2}+\sqrt{3})x.$$

The main observation is that entries of $[T]_{\mathcal{B}\mathcal{B}}$ are integers. Indeed, for every $x\in\mathcal{B}$ the number $(\sqrt{2}+\sqrt{3})x$ is a linear combination of elements of $\mathcal{B}$ with integer coefficients.

Let $p(\lambda)=\det(T-\lambda I)$ be the characteristic polynomial of T. Since $[T]_{\mathcal{B}\mathcal{B}}$ has integer entries, the coefficients of p are integers. Furthermore p is a monic polynomial. By Cayley–Hamilton theorem $p(T)=0$. Since T is a multiplication by $\sqrt{2}+\sqrt{3}$, the linear transformation $p(T)\colon V\to V$ is multiplication by $p(\sqrt{2}+\sqrt{3})$. Hence, $p(\sqrt{2}+\sqrt{3})=0$, and so $\sqrt{2}+\sqrt{3}$ is an algebraic integer.

[*] These notes are available from the course webpage, and directly from `http://www.borisbukh.org/MatrixTheory13/notes_alg_integers.pdf`

General case: $\alpha+\beta$

In the proof of general case, we dodge the issue of whether the set $\mathcal{B}$ (defined below) is linearly independent over $\mathbb{Q}$. This complicates the argument slightly, as instead of defining T we define a slightly more involved operator.

Let α and β be algebraic integers of degrees m and n, respectively. Say

$$\begin{aligned} \alpha^m &= \sum_{r=0}^{m-1} a_r \alpha^r, \\ \beta^n &= \sum_{s=0}^{n-1} b_s \alpha^r, \end{aligned} \tag{1}$$

where a's and b's are integers. Define the set $\mathcal{B} = \{\alpha^i\beta^j : 0 \le i < m-1,\ 0 \le j < n-1\}$. The set $\mathcal{B}$ need not be linearly independent (for example if $\alpha=\beta$).

Think of coordinates of $\mathbb{C}^{mn}$ as being indexed by pairs (i,j) of numbers that satisfy $0 \le i < m$ and $0 \le j < n$. Let $\vec{e}_{i,j}$ for $0 \le i < m-1$ and $0 \le j < n-1$ be the basis vectors. Define $T' \colon \mathbb{C}^{mn} \to \mathbb{C}^{mn}$ by

$$T'\vec{e}_{i,j} = \begin{cases} \vec{e}_{i+1,j} + \vec{e}_{i,j+1} & \text{if } i < m-1,\ j < n-1 \\ \vec{e}_{i+1,j} + \sum_{s=0}^{n-1} b_s \vec{e}_{i,s} & \text{if } i < m-1,\ j = n-1 \\ \sum_{r=0}^{m-1} b_r \vec{e}_{r,j} + \vec{e}_{i,j+1} & \text{if } i = m-1,\ j < n-1 \\ \sum_{r=0}^{m-1} b_r \vec{e}_{r,n-1} + \sum_{s=0}^{n-1} b_s \vec{e}_{m-1,s} & \text{if } i = m-1,\ j = n-1. \end{cases}$$

The formula is motivated by writing $(\alpha+\beta)\alpha^i\beta^j$ into a linear combination of elements of $\mathcal{B}$ using relations (1).

Note that the entries of the matrix expressing T' in the standard basis are integers. So, the characteristic polynomial of T' is an integer polynomial whose leading coefficient is $(-1)^{mn}$. Since eigenvalues are roots of the characteristic polynomial, it follows that the eigenvalues are algebraic integers. We will show that $\alpha+\beta$ is an eigenvalue.

Consider $T' - (\alpha+\beta)I$, and consider the linear transformation $S \colon \mathbb{C}^{mn} \to \mathbb{C}$ defined on the basis elements by $S(\vec{e}_{i,j}) = \alpha^i\beta^j$. It is clear that for every $\vec{v} \in \mathbb{C}^{mn}$ we have $\bigl(T' - (\alpha+\beta)I\bigr)\vec{v} \in \operatorname{Ker} S$. Hence $\dim \operatorname{Ran} S = 1$, it follows by rank-nullity theorem that

$$\begin{aligned} \dim \operatorname{Ker}\bigl(T' - (\alpha+\beta)I\bigr) &= mn - \dim \operatorname{Ran}\bigl(T' - (\alpha+\beta)I\bigr) \\ &\ge mn - \operatorname{Ker} S = \dim \operatorname{Ran} S = 1. \end{aligned}$$

Hence $\operatorname{Ker}\bigl(T' - (\alpha+\beta)I\bigr)$ contains a non-zero vector, and so $\alpha+\beta$ is an eigenvalue of T'.