Algebraic numbers

Here we will see in a sequence of exercises how to show that certain numbers are algebraic. Recall that $\alpha \in \mathbb{C}$ is an *algebraic number* if it is a root of a polynomial with integer coefficients. If in addition the polynomial can be chosen to be *monic* then α is an *algebraic integer*.

For example, $\sqrt{2}$ and $\sqrt[3]{5}$ are algebraic integers, roots of polynomials x^2-2 and x^3-5 respectively. On the other hand, $\frac{1}{2}$ is an algebraic number, but not an algebraic integer.

Exercise 1. *If $\alpha \neq 0$ is an algebraic number, show that $-\alpha, \frac{1}{\alpha}$ are also algebraic. Also show that rational multiples of α are algebraic.*

What's not obvious is that numbers like $\sqrt{2}+\sqrt{3}+\sqrt{5}+\sqrt{7}$ are algebraic. If there aren't too many roots you can square and simplify, but with 4 roots it seems to get out of hand (you can still pull it off though!). But then imagine $\sqrt{2}+\sqrt[3]{3}+\sqrt[5]{5}+\sqrt[7]{7}$!

If $z_1, \cdots, z_m$ are complex numbers, define $V_{\mathbb{Q}} = V_{\mathbb{Q}}(z_1, \cdots, z_m)$ as the set of all rational linear combinations of $z_1, \cdots, z_m$.

Exercise 2. *Show that $V_{\mathbb{Q}}$ is a finite dimensional vector space over $\mathbb{Q}$.*

We are particularly interested in finding $V_{\mathbb{Q}}$ such that the given $\alpha \in \mathbb{C}$ acts on it by multiplication.

Definition 3. *$V_{\mathbb{Q}}$ is α-invariant if $v \in V_{\mathbb{Q}}$ implies $\alpha v \in V_{\mathbb{Q}}$.*

Exercise 4. *Prove that $V_{\mathbb{Q}}(1, \sqrt{2})$ is $\sqrt{2}$-invariant. Prove that $V_{\mathbb{Q}}(1, \sqrt[3]{5}, \sqrt[3]{5}^2)$ is $\sqrt[3]{5}$-invariant.*

Exercise 5. *Suppose that for every j we have $\alpha z_j \in V_{\mathbb{Q}}$. Prove that $V_{\mathbb{Q}}$ is α-invariant.*

Exercise 6. *If α is a root of the integral polynomial $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, show that $V_{\mathbb{Q}}(1, \alpha, \alpha^2, \cdots, \alpha^{n-1})$ is α-invariant.*

This exercise proves one half of the following theorem.

Theorem 7. *$\alpha \in \mathbb{C}$ is an algebraic number if and only if there exists some nonzero $V_{\mathbb{Q}}$ (finite dimensional rational vector subspace of $\mathbb{C}$) which is α-invariant.*

For the second half we will fix a basis of $V_{\mathbb{Q}}$, say $w_1, \cdots, w_n$. Let M be the $n \times n$ matrix of the linear map $V_{\mathbb{Q}} \to V_{\mathbb{Q}}$ given by $v \mapsto \alpha v$.

Exercise 8. *Prove that this is a linear map.*

Exercise 9. *Compute M for the examples above. Also compute the characteristic polynomial of M.*

Now M has a characteristic polynomial, which has rational coefficients (why?) and degree n. Recall the Cayley-Hamilton theorem, which says that M satisfies its characteristic polynomial. Thus we have an identity

$$M^n + a_{n-1}M^{n-1} + \cdots + a_1 M + a_0 I = 0$$

with a_i rational.

Exercise 10. *Show that $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$*

As a hint, what is the matrix of the linear map represented by the multiplication by the number on the left hand side?

Now this proves that α is algebraic, by clearing the denominators. The theorem is then proved.

Here is the main application.

Theorem 11. *If α, β are two algebraic numbers, then so are $\alpha + \beta$ and $\alpha\beta$. As a consequence, the set of algebraic numbers in $\mathbb{C}$ is a field, called algebraic closure of $\mathbb{Q}$, and is denoted $\overline{\mathbb{Q}}$.*

Exercise 12. *Suppose $V_{\mathbb{Q}} = V_{\mathbb{Q}}(z_1, \cdots, z_m)$ and $W_{\mathbb{Q}} = V_{\mathbb{Q}}(w_1, \cdots, w_k)$ are α-invariant and β-invariant nontrivial finite dimensional rational spaces as above, respectively. Form the new space*

$$U_{\mathbb{Q}} = V_{\mathbb{Q}}(z_1 w_1, z_1 w_2, \cdots, z_m w_k)$$

and show that it is both α-invariant and β-invariant. Deduce the theorem.

Exercise 13. *For every $n = 1, 2, 3, \cdots$ the number $\cos\frac{2\pi}{n}$ is algebraic.*

Hint: it is the average of two roots of $x^n - 1$.

Remark 14. *A similar discussion works for algebraic integers. The difference is that now we have to work with the space $V_{\mathbb{Z}}$ of* **integral** *linear combinations of the given complex numbers. Then we have to use linear algebra over $\mathbb{Z}$ to find an integral basis, and see that the entries in M and the coefficients of the characteristic polynomial are all in $\mathbb{Z}$. The conclusion is that if α, β are algebraic integers, so are $\alpha + \beta$ and $\alpha\beta$. It is no longer true that $\alpha \neq 0$ alg. integer implies $\frac{1}{\alpha}$ is an algebraic integer (think of $\frac{1}{2}$). So the conclusion is that the set of algebraic integers is a subring of $\mathbb{C}$.*