Math 204A (Number Theory), UCSD, fall 2020
Notes on algebraic numbers and algebraic integers

An *algebraic number* is an element $\alpha \in \mathbb{C}$ for which there exists a nonzero polynomial $P(x) \in \mathbb{Q}[x]$ such that $P(\alpha) = 0$.

A *number field* is a subfield of $\mathbb{C}$ which is finite-dimensional as a $\mathbb{Q}$-vector space.[1]

- Any finite set of algebraic numbers is contained in some number field.
- Conversely, an element $\alpha \in \mathbb{C}$ is an algebraic number if and only if $1, \alpha, \alpha^2, \ldots$ all belong to some finite-dimensional $\mathbb{Q}$-vector subspace of $\mathbb{C}$. (Hint: any linear dependence relation gives rise to a polynomial with α as a root.)
- The set $\overline{\mathbb{Q}}$ of algebraic integers is a subfield of $\mathbb{C}$. That is, $\overline{\mathbb{Q}}$ is closed under addition, subtraction, multiplication, and division. (This follows from the previous statements.)
- For any algebraic number α, there is a unique monic (leading coefficient 1) polynomial $P(x) \in \mathbb{Q}[x]$ of minimal degree such that $P(\alpha) = 0$. It is called the *minimal polynomial* of α. (Hint: the set of polynomials which vanish on α is a nonzero ideal of $\mathbb{Q}[x]$. Use Euclidean division to show that this ideal is principal.)
- If $\alpha \in \mathbb{C}$ is a root of a nonzero polynomial $P(x) \in \overline{\mathbb{Q}}[x]$, then $\alpha \in \overline{\mathbb{Q}}$. (Hint: first put all of the coefficients of P into a number field.)
- The set $\overline{\mathbb{Q}}$ is countable; that is, it can be put into bijection with $\mathbb{Z}$, but not with $\mathbb{R}$ or $\mathbb{C}$.

An *algebraic integer* is an element $\alpha \in \mathbb{C}$ for which there exists a monic polynomial $P(x) \in \mathbb{Z}[x]$ such that $P(\alpha) = 0$.

- Any $\alpha \in \mathbb{Q}$ is an algebraic number. It is an algebraic integer if and only if it is in $\mathbb{Z}$. (Hint: use the rational root theorem. This is a special case of Gauss's lemma; see below.) We will sometimes use the term[2] *rational integer* to refer to elements of $\mathbb{Z}$.
- For any algebraic number α, α is an algebraic integer if and only if its minimal polynomial belongs to $\mathbb{Z}[x]$. (Hint: use Gauss's lemma on the content of polynomials.)
- For any algebraic number α, α is an algebraic integer if and only if $1, \alpha, \alpha^2, \ldots$ all belong to a finitely generated $\mathbb{Z}$-submodule of $\mathbb{C}$. (Hint: if there is such a submodule, then the submodules generated by $1, \alpha, \ldots, \alpha^n$ for successive values of n must eventually stabilize.)

[1] More accurately, a number field is an *abstract* field of characteristic 0 which is finite-dimensional as a $\mathbb{Q}$-vector space. What I just defined should really be called an *embedded* number field; we'll come back to this in a few lectures.

[2] This linguistic construction is an example of a *retronym*.

- The set $\overline{\mathbb{Z}}$ of algebraic integers is a subring of $\mathbb{C}$. That is, $\overline{\mathbb{Z}}$ is closed under addition, subtraction, and multiplication, but not division.
- If $\alpha \in \mathbb{C}$ is a root of a nonzero monic polynomial $P(x) \in \overline{\mathbb{Z}}[x]$, then $\alpha \in \overline{\mathbb{Z}}$.