Lecture 1

Algebraic Number

We call $a \in \mathbb{C}$ an <u>algebraic number</u> if $\exists$ a non-zero $f \in \mathbb{Q}[x]$ s.t. $f(a) = 0$

Def: For any "ring" A by $A[x]$ we mean the "polynomial ring" with coefficients in A, i.e. $A[x] = \left\{ a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \;\middle|\; n \in \mathbb{N},\ a_0, \dots, a_n \in A \right\}$

Exemple: $\mathbb{C}[x]$, $\mathbb{Z}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$ etc.

Example: i) $\sqrt{2}$ is algebraic number

$x^2 - 2 = 0$ is solved by $\sqrt{2}$

ii) $3i$ is alg. no. as $x^2 + 9 = 0$ has root $3i$

iii) $\frac{-1+\sqrt{3}i}{2}$ is alg no. as $\left(\frac{-1+\sqrt{3}i}{2}\right)^3 = 1$.

Algebraic integers

We call $a \in \mathbb{C}$ an *algebraic integer* if $\exists\ 0 \neq f \in \mathbb{Z}[x]$ monic s.t. $f(a) = 0$.

A polynomial is called *monic* if its leading coefficient is 1.

Ex: $a = \sqrt{2}$

Non-ex: $a = \frac{1}{\sqrt{2}}$. It is algebraic numbers as $x^2 - \frac{1}{2} = 0$ is solved by $1/\sqrt{2}$. But is there a monic polynomial with integer entries whose one root is $1/\sqrt{2}$?

Non-ex: π & e are not even algebraic number.

Def: The complex numbers that are not algebraic are called *trancendental*.

<u>Prop</u>: A rational number is an algebraic integer iff it is an integer.

<u>Pf</u>: "$\Rightarrow$" Every integer is trivially an algebraic integer.

"$\Leftarrow$" Let $r = \frac{s}{t}$, $GCD(s,t) = 1$ be an algebraic integer. We need to show that $r \in \mathbb{Z}$, in other words $t = 1$.

By definition r satisfies

$$r^n + c_{n-1} r^{n-1} + \cdots + c_0 = 0$$

for some $c_0, c_1, \ldots, c_{n-1} \in \mathbb{Z}$.

Substituting $r = \frac{s}{t}$ & multiplying by t^n we obtain

$$s^n + \left(c_{n-1} s^{n-1} t + \cdots + c_0 t^n\right) = 0$$

$$\Rightarrow s^n + t\left(c_{n-1} s^{n-1} + \cdots c_0 t^{n-1}\right) = 0$$

Thus $t \mid s^n$. But $GCD(s,t) = 1$

This is only possible if $t = 1$.

(To see this let p a prime and $p \mid t$

$\Rightarrow p \mid s^n \Rightarrow p \mid s \Rightarrow GCD(s,t) \geq p$
≥ 2)

.

<u>Def</u>: Let a be an algebraic number. We call $f \in \mathbb{Q}[x]$ to be <u>the minimal polynomial</u> of a if

- f is monic.
- $f(a) = 0$
- f has the minimum degree among all polynomials with the above property.

<u>Lemma</u>: Minimal polynomial is unique.

<u>Pf</u>: Let f_1 & f_2 be two minimal polynomials of a. Let $g := f_1 - f_2$

Obviously, $g(a) = f_1(a) - f_2(a) = 0$

and g has strictly smaller degree

than degree of f_1 (and f_2). So

$$g(x) = a_\ell x^\ell + \cdots + a_0 \ ; \quad a_\ell \neq 0$$

and $\quad \ell < \deg(f_1) = \deg(f_2)$

But $\dfrac{g(x)}{a_\ell}$ satisfies requirements of the minimal polynomials. Hence $g = 0$ & $f_1 = f_2$.

<u>Ex</u>: Minimal polynomial of $\sqrt{2}$ is $x^2 - 2$. Indeed, if there is a degree one polynomial $ax + b$ $a, b \in \mathbb{Q}$, s.t. $a\sqrt{2} + b = 0$ then $\sqrt{2} = -\frac{b}{a}$ $\in \mathbb{Q}$ ↯.

<u>Lemma</u>: Let f be the minimal polynomial of a & $g(a) = 0$. Then $f \mid g$

<u>Pf</u>: Euclid's algorithm for polynomials $\exists\, q, r \in \mathbb{Q}[x]$ with $\deg(r) < \deg(f)$

s.t. $g(x) = q(x) f(x) + r(x)$

So if $g(a) = 0$ and as $f(a) = 0$ we have. $r(a) = 0$. But as $\deg(r) < \deg(f)$ it contradicts minimality of f unless $r = 0$.
In others words $g = qf \Rightarrow f \mid g$.

Theorem (Gauss's lemma)

An algebraic number is an algebraic integer if and only if its minimal polynomial $\in \mathbb{Z}[x]$.

Quadratic number field

We call a number $a \in \mathbb{C}$ to be quadratic if the minimal polynomial of a has degree 2.

Ex: $a = \sqrt{2}$, $\sqrt{3}$, $\sqrt{d}$, $d \in \mathbb{N}$
$d \neq$ square.

$\frac{\sqrt{3}-1}{2}$, $-3i$ ...

The set $\mathbb{Q}(a) := \{ f(a) \mid f \in \mathbb{Q}[x] \}$ is a "field". It is the minimal field $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ which contains a. If a is quadratic we call $\mathbb{Q}(a)$ to be a quadratic number field. One has

$$\mathbb{Q}(a) = \{ s + ta \mid s, t \in \mathbb{Q} \}.$$

Def: The set of algebraic integers in a field is denoted by integer ring or ring of integers of that field.

Ex: If $d \in \mathbb{Z}$ square free. The set of algebraic integers in $\mathbb{Q}(\sqrt{d})$ is called the ring of integers of $\mathbb{Q}(\sqrt{d})$.