Last time: $\mathbb{Z}[i]$ primes

Defn 1) A number field is a subfield of $\mathbb{C}$ that is fin dim'l as a $\mathbb{Q}$-vs e.g. $\mathbb{Q}(i)$

2) An algebraic number is a complex # that is the root of a poly w/ $\mathbb{Q}$ coeff

Obs if K is a num field every elt is an alg #

Pf if $x \in K$ given $1, x, x^2, \ldots \in K$

(since K fin dim, this list has to be lin dep / $\mathbb{Q}$

$\Rightarrow$ can write linear dependy that is a poly in $\mathbb{Q}$ which x satisfies!

Obs If R is a subring of $\mathbb{C}$ containing $\mathbb{Q}$ + fin dim'l as a $\mathbb{Q}$ vs $\Rightarrow$ R is a field.

Pf let $x \in R$ nonzero,

Consider $m_x : R \longrightarrow R$

$a \longmapsto xa$

This is $\mathbb{Q}$ linear (distributivity)

It is injective since R is a domain (as $\mathbb{C}$ is a domain)

As R is fin dim as a $\mathbb{Q}$ vs $\Rightarrow$ m_x is surj too

$\Rightarrow$ $\exists\ b \in R$ so $bx = 1$ $\Rightarrow b = x^{-1}$

So R is a field!

Obs if $x \in \mathbb{C}$ is an alg # then

$\mathbb{Q}[x] = \mathbb{Q}\text{-span}(1, x, \ldots) \longrightarrow$ ring

(sp check) $\uparrow$ is a number field.

Pf By assump $\exists$ nonzero $f(T) \in \mathbb{Q}[T]$

s.t. $f(x) = 0 \Rightarrow x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$

$\Rightarrow x^n \in \text{span}(x^{n-1}, \ldots, 1)$ & $x^{n+1} \in \text{span}(x^n, \ldots, 1) = \text{sp}(x^{n-1}, \ldots, 1)$

$\Rightarrow$ continuing $x^i \in \mathrm{sp}(1, \dots, x^{n-1}) \quad \forall i \geq n$

$\Rightarrow \dim_{\mathbb{Q}} \mathbb{Q}[x] \leq n$

By obs 2: this is a number field

$\mathbb{Q}[x] \subseteq \mathbb{Q}(x)$ always, by abv $\mathbb{Q}(x) \subseteq \mathbb{Q}[x]$

So if x alg $\mathbb{Q}[x] = \mathbb{Q}(x)$ (in fact iff)

Thm The set of alg #'s forms a subfield of $\mathbb{C}$

Pf If x is algebraic $\Rightarrow \frac{1}{x}$ is algebraic

1) $\frac{1}{x} \in \mathbb{Q}[x]$ ↪ number field $\Rightarrow$ obs 1 gives all elts of num field are alg.

Say x, y alg #s

WTS $x+y, xy$ are alg #s

Consider $\mathbb{Q}[x,y] = \mathbb{Q}\text{-sp}(x^i y^j \mid i,j \geq 0) \subseteq \mathbb{C}$

↪ this is fin dim by earlier arg

i.e. x, y satisfy poly of n, m resp.

$\Rightarrow \mathbb{Q}[x,y]$ sp by $x^i y^j \quad 0 \leq i,j$ & $i \leq n-1, j \leq m-1$

So, $\mathbb{Q}[x,y]$ is a num field

$\Rightarrow x+y, x \cdot y$ are alg

Rmk Say $a \in \mathbb{C}$ is an alg #

$\exists!$ monic poly $f(T) \in \mathbb{Q}(T)$ of min deg s.t. $f(a) = 0$

Moreover, if $g(T) \in \mathbb{Q}(T)$ so $g(a) = 0$

$\Rightarrow f(T) \mid g(T)$

Pf $\mathrm{ev}_a : \mathbb{Q}[T] \to \mathbb{C}$, $g(T) \mapsto g(a)$

$f(T)$ is the unique monic gen of $\ker \mathrm{ev}_a$ ideal

↪ $\ker \mathbb{Q}[T]$ is a PID

↪ $\mathbb{Q}^\times$ are the units

↪ Min poly of a

Fact $\frac{\mathbb{Q}[T]}{(f(T))} \cong \mathbb{Q}[a] = \mathbb{Q}(a)$ ↳ first iso thm

↳ this as earlier (irreducible).

$\dim_{\mathbb{Q}} \mathbb{Q}[a] = \deg f(T)$

Special Case $a = \sqrt{-1}$ $f(T) = T^2+1$

$\mathbb{Q}[a] = \mathbb{Q}(a)$ is a 2-D v.sp!

Def A $\mathbb{C}$ number a is an algebraic integer if $\exists$ monic poly $0 \neq f(T) \in \mathbb{Z}[T]$ s.t. $f(a)=0$

Eg A rat'l number that is an alg int is an ord integer!

Fact The set of all algebraic integers is a subring of $\mathbb{C}$ (similar to abv using $\mathbb{Z}$-modules not $\mathbb{Q}$-vs)

If K is a number field we defn

$\mathcal{O}_K = \{\text{alg ints that are in } K\}$

This is a subring of K, called the ring of integer of K

Eg If $\dim_{\mathbb{Q}}(K) = 2$ then

$K = \mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z}$ sq free

$$\mathcal{O}_K = R_d = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2,3 \bmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \bmod 4 \end{cases}$$

Major Prob Understand factorization in these number rings.

for which K is $\mathcal{O}_K$ a UFD?

Eg $K = \mathbb{Q}[\sqrt{d}]$ for $d<0$ & d sq-free

$\Rightarrow$ $\mathcal{O}_K$ is a UFD for 9(?) values of d

Recall An ideal I is prime if $xy \in I \Rightarrow x \in I$ or $y \in I$

Fact Every max'll ideal is prime

Ex $\mathbb{Z}[\sqrt{-5}]$ $\quad 6 = 2 \cdot 3 = (1+\sqrt{-5})(1+\sqrt{-5})$

$(2, 1+\sqrt{-5})$ is a max ideal (all nonzero ideals in # fields are max'l)

If I, J are ideals

IJ = ideal gen'd by xy w/ $x \in I$ $y \in J$

Ex w/ princ ideals: $(x)(y) = (xy)$

Thm Let k a # field & $I \subseteq \mathcal{O}_k$, $I \neq 0$

Then $\exists!$ factorization

$$I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$$

where $\mathfrak{p}_i$'s are distinct prime ideals $e_i \geq 1$

Idea of fractional ideal of $\mathcal{O}_k$

(Ex frac ideal of $\mathbb{Z}$ is $\frac{1}{2}\mathbb{Z}$)

↳ frac ideals form a group under $\times$ mult (X)

$\exists$ subgrp $Y \subseteq X$ of principle frac ideals.

The ideal class grp of k is $Cl(k) = X/Y$

Facts 1) TFAE

- $\mathcal{O}_k$ PID
- $\mathcal{O}_k$ UFD
- $Cl(k)$ is triv.

2) $Cl(k)$ is finite