Arithmetic Dynamics Talk 1

§ Number Fields

- A field K is called a number field if it is a finite extension of $\mathbb{Q}$.

Ex: $\mathbb{Q}(\sqrt{5})$
$\mathbb{Q}(i)$

(over $\mathbb{Q}$)

Def A number field is Galois, if it is the splitting field extension of an irreducible $f \in \mathbb{Z}[x]$.
That is K is Galois if $K = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$ where $\alpha_1, \dots, \alpha_n$ are the roots of f.

Ex. $\mathbb{Q}(\sqrt{5})$ is Galois
$\mathbb{Q}(\sqrt[3]{2})$ is NOT Galois but $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$ is.

Def. Given α algebraic (i.e. $[\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$) α is called integral if it is the root of some monic $f \in \mathbb{Z}[x]$.

Ex. $\frac{1+\sqrt{5}}{2}$ is integral since its the root of $x^2 + x + 1$.

Def Given a number field, K, its ring of integers $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K, i.e.

$$\mathcal{O}_K = \{\alpha \in K \mid \alpha \text{ integral}\}.$$

Ex $K = \mathbb{Q}(\sqrt{5})$ $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$
$K = \mathbb{Q}(\sqrt{3})$ $\mathcal{O}_K = \mathbb{Z}[\sqrt{3}]$.

Fact. Given $[K:\mathbb{Q}] = n$, $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module ~~with~~ of rank n.

Fact Given a number field K, $\mathcal{O}_K$ is a Dedekind domain. This means we have unique prime decomposition.

Lemma Let $\mathcal{O}_K$ be the ring of integers of a number field. Then every ideal $\mathfrak{q} \leq \mathcal{O}_K$ can be written uniquely as

$$\mathfrak{q} = \prod_i \mathfrak{p}_i^{e_i}$$

where $\mathfrak{p}_i$ are distinct prime ideals of $\mathcal{O}_K$ and $e_i \in \mathbb{N}$.

Ex $K = \mathbb{Q}$, $\mathcal{O}_K = \mathbb{Z}$, prime ideals of $\mathbb{Z} \leftrightarrow$ prime numbers. (fund. thm of arithmetic).

Ex. $K = \mathbb{Q}(i)$ $\quad (2) = (1+i)^2$
$\mathcal{O}_K = \mathbb{Z}[i]$.

Note: $\mathcal{O}_K$ is not necessarily a PID, i.e. not all prime ideals are principal.
So $\mathcal{O}_K$ is not necessarily a UFD.

Ex

§ Local Fields

Def Let p be a prime number we define $|\cdot|_p : \mathbb{Q} \to \mathbb{Z}$ the p-adic abs. value as follows.
~~Let $a/b \in \mathbb{Q}$ s.t. a, b coprime integers~~
Let $n \in \mathbb{Z}$. $v_p(n)$ is the largest m s.t. $p^m | n$.
i.e. $n = \prod_p p^{v_p(n)}$.

Given $a/b \in \mathbb{Q}$ a, b coprime integers
$v_p(a/b) = v_p(a) - v_p(b)$ the p-adic valuation

Then for $q \in \mathbb{Q}$
$|q|_p = p^{-v_p(q)}$.

Ex $v_5(5) = 1 \Rightarrow |5|_5 = 1/5$

$v_5(\frac{1}{5}) = -1 \Rightarrow |1/5|_5 = 5$

$v_5(\frac{20}{3}) = 1 \Rightarrow |20/3|_5 = 1/5$.

Def. $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ wrt $|\cdot|_p$.

Lemma $\mathbb{Q}_p = \{ \sum_{i=n}^{\infty} a_i p^i \mid a_i \in \{0, \dots, p-1\}, n \in \mathbb{Z} \}$.

§ Abs. Values and Local Fields

Def Given a field F an abs. value is a function $|\cdot| : F \to \mathbb{Z}$ s.t.

- $|x| = 0 \iff x = 0$
- $|xy| = |x| \cdot |y| \quad \forall x, y \in F$
- $|x+y| \leq |x| + |y| \quad \forall x, y \in F$.

Def An abs. value $|\cdot| : F \to \mathbb{R}_{\geq 0}$ is called non-archemedian if it satisfies the ultrametric inequality:

$$|x+y| \leq \max(|x|, |y|)$$

If it isn't non-archimedian we call an abs. value archimedian.

Ex/Def Let p be a prime number. p-adic valuation.

Define $v_p : \mathbb{Q} \to \mathbb{Z}$, as follows.

Given $n \in \mathbb{Z}$ $v_p(n)$ is the largest $m \in \mathbb{Z}$ s.t. $p^m | n$.

i.e. $n = \prod_p p^{v_p(n)}$

Given $q \in \mathbb{Q}$ we may write q as a/b $a, b \in \mathbb{Z}$ coprime.

$v_p(q) = v_p(a) - v_p(b)$.

Define the p-adic abs. value $|\cdot|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ as

$$|n|_p = p^{-v_p(n)}.$$

Ex $v_5(5) = 1 \Rightarrow |5|_5 = 1/5$

$v_5(1/5) = -1 \Rightarrow |5|_5 = 5$

$v_5(20/3) = 1 \Rightarrow |20/3|_5 = 1/5$.

Lemma For all primes p $|\cdot|_p$ is a non-archimedian abs. value.

Pf - exercise.

Ex Let $|\ |_\infty$ denote the usual abs. value on $\mathbb{C}$.
i.e. $|a+bi|_\infty = \sqrt{a^2+b^2}$. This is an archimedian abs. value.

Def ~~The p-adic numbers $\mathbb{Q}_p$ are~~ The field $\mathbb{Q}_p$ is defined to be the completion of $\mathbb{Q}$ wrt $|\cdot|_p$.

Recall $\mathbb{R}$ completion of $\mathbb{Q}$ wrt $|\cdot|_\infty$

$$\mathbb{Q} \xrightarrow{|\cdot|_\infty} \mathbb{R}, \qquad \mathbb{Q} \xrightarrow{|\cdot|_p} \mathbb{Q}_p$$

§Local Fields

Def A local field is a field K such that
- $K \cong \mathbb{R}$ or $\mathbb{C}$ (arch)
- $K \cong \mathbb{F}_{p^n}((t))$ (non-arch)
- K is a finite ext. of $\mathbb{Q}_p$. (non-arch)

↳ ALWAYS comes with an ~~abs~~ associated abs. value.

Def Let $(K, |\cdot|)$ be a local field, its ring of integers $\mathcal{O}_K$ is

$$\mathcal{O}_K = \{ x \in K \mid |x| \leq 1 \}$$

Lemma. $\mathcal{O}_K$ is integrally closed in K.

Ex/Pf Given $K = \mathbb{Q}_p$, $\mathcal{O}_K = \mathbb{Z}_p$ the p-adic integers.

~~$\mathbb{Z}_p \cong \varprojlim \mathbb{Z}/p^n\mathbb{Z}$~~

$$\mathbb{Z}_p = \{ x \in \mathbb{Q}_p \mid |x|_p \leq 1 \}$$

It follows that

$$\{ \tfrac{a}{b} \in \mathbb{Q} \mid (a,b) = 1, \ p \nmid b \} \subseteq \mathbb{Z}_p.$$

i.e. $5 \in \mathbb{Z}_5$

$\frac{20}{3} \in \mathbb{Z}_5$

$\frac{1}{5} \notin \mathbb{Z}_5$.

Lemma $\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$.

It follows that

$$\mathbb{Z}_p = \{ \sum_{i=0}^{\infty} a_i p^i \mid a_i \in \{0, 1, \cdots, p-1\} \}$$

&

$$\mathbb{Q}_p = \{ \sum_{i=n}^{\infty} a_i p^i \mid a_i \in \{0, \cdots, p-1\} \ n \in \mathbb{Z} \}.$$

Lemma ~~Given K a local field, $\mathcal{O}_K$ is a~~ $\mathbb{Z}_p$ is the closure of $\mathbb{Z}$ in $\mathbb{Q}_p$ wrt $|\cdot|_p$.

Lemma Given K a local field $\mathcal{O}_K$ is a principal local ring (has a unique maximal ideal).

Ex. $\mathbb{Z}_p$ has unique maximal ideal (p). p uniformizer

~~The unique max~~ We call π a uniformizer of K if (π) is the unique max. ideal of $\mathcal{O}_K$

Why are local fields helpful?

Hensel's Lemma

Let $f \in \mathbb{Z}[x]$. Let $a \in \mathbb{Z}$ such that

$$f(a) \equiv 0 \bmod p^n \qquad n \text{ even, odd.}$$

$$f'(a) \not\equiv 0 \bmod p^{\left(\frac{n}{2} \text{ or } \frac{n+1}{2}\right)}.$$

Then there exists a unique element $\alpha \in \mathbb{Z}_p$ such that $\alpha \equiv a \bmod p^n$ and $f(\alpha) = 0$.

Ex Let p be an odd prime s.t. $p \equiv 1 \bmod 4$.

Then $(-1/p) = 1$, i.e. $x^2 \equiv -1 \bmod p$ has a solution. Call this a. Let $f(x) = x^2 + 1$.

$f(a) \equiv 0 \bmod p$

$f'(a) = 2a \not\equiv 0 \bmod p$

$\Rightarrow \sqrt{-1} \in \mathbb{Z}_p$.

Since $\mathbb{Q} \subset \mathbb{Q}_p$ if number theorists want rational solutions to an equation they first often check if there are solutions in $\mathbb{Q}_p$ $\forall p$.

Ramification

Let K be a number field.

Recall $\mathcal{O}_K$ has unique prime factorisation

Therefore all rational primes p we have unique $\mathfrak{P}_1, \dots, \mathfrak{P}_n$ s.t.

$$p\mathcal{O}_K = \prod_i \mathfrak{P}_i^{e_i} \qquad \mathfrak{P}_i \text{ primes in } \mathcal{O}_K.$$

Fact If $K/\mathbb{Q}$ Galois $e_1 = e_2 = \dots = e_n$.

If $p\mathcal{O}_K = \prod_{i=1}^{n} \beta_i^{e_i}$ then we use the notation

$\beta_i \mid p$. or "β_i ~~ab~~above p".

Def Let K be a number field and p a rational prime we say p ramifies in K if where $p = \prod \beta_i^{e_i}$ $e_i > 1$ for some i.

Ex $K = \mathbb{Q}(i)$ $(2) = (1+i)^2$, → 2 ramifies in $\mathbb{Q}(i)$.

Lemma Given $K/\mathbb{Q}$ only a finite number of primes ramify in K.

Ex Only 2 ramifies in $\mathbb{Q}(i)/\mathbb{Q}$.