Review of some algebraic number theory 15/3/19

(Loosely based on a lecture by Dick Gross.)

A <u>number field</u> is a finite extension of $\mathbb{Q}$, $\deg = n = \dim K/\mathbb{Q}$.

$$\begin{array}{c} K \\ | \\ \mathbb{Q} \end{array}$$

"degree"

$$\begin{array}{ccc} K & \supset & \mathcal{O} \\ | & & | \\ \mathbb{Q} & \supset & \mathbb{Z} \end{array}$$

$\mathcal{O}$ = ring of integers

$= \{x \mid x \text{ satisfies a monic polynomial}\}$.

⓪ $K = \mathbb{Q}(\sqrt{2})$ then $\mathcal{O} = \mathbb{Z}[\sqrt{2}]$, $K = \mathbb{Q}(i)$, $\mathcal{O} = \mathbb{Z}[i]$.

<u>Exercise</u>: ① $K = \mathbb{Q}(\sqrt{5})$, then $\mathcal{O} = \mathbb{Z}[\phi]$ where $\phi = \frac{1+\sqrt{5}}{2}$.

② $K = \mathbb{Q}(\sqrt{\alpha})$ then $\mathcal{O} = \begin{cases} \mathbb{Z}\left(\frac{1+\sqrt{\alpha}}{2}\right) & \text{if } \alpha \equiv 1 \bmod 4 \\ \mathbb{Z}(\sqrt{\alpha}) & \text{otherwise.} \end{cases}$

$\mathcal{O}$ is a free $\mathbb{Z}$-module of rank n.

<u>Thm</u> $\mathcal{O}$ is a Dedekind domain $\left(\begin{array}{c}\text{normal, Noetherian,} \\ \text{Krull dimension one}\end{array}\right)$.

$$\begin{array}{c} K \\ | \\ \mathbb{Q} \end{array}$$

given $x \in K$, get a $\mathbb{Q}$-linear map $x\cdot$

$\mathrm{Tr}(x) := \mathrm{Tr}(x\cdot)$ $\quad \mathrm{Tr}: K \longrightarrow \mathbb{Q}$

$\mathrm{Norm}(x) := \mathrm{Det}(x\cdot)$. $\quad \mathrm{Nm}: K^\times \longrightarrow \mathbb{Q}^\times$

$\rightsquigarrow$ gives a bilinear form $K \times K \longrightarrow \mathbb{Q}$

$(x, y) \longmapsto \mathrm{Tr}(xy)$.

Non-degenerate because $\mathrm{Tr}(1) = n$, hence $\mathrm{Tr}(xx^{-1}) = n \neq 0$.

Any elt of $\mathcal{O}$ satisfies a monic polynomial

$\Rightarrow$ $Tr : \mathcal{O} \times \mathcal{O} \to \mathbb{Z}$. $d =$ <u>Discriminant</u> $= \det(Tr(\alpha_i \alpha_j))$

where $\alpha_1, \dots, \alpha_j$ is a $\mathbb{Z}$-basis for $\mathcal{O}$.

<u>E.g.</u> $\mathcal{O} = \mathbb{Z}[i]$, $\begin{array}{c|cc} & 1 & i \\ \hline 1 & 2 & 0 \\ i & 0 & -2 \end{array}$

Close relative of discriminant of a polynomial.

$\Rightarrow$ discriminant $= -4$.

Useful to consider dual lattice $\mathcal{O}^\vee = \{ x \in K \mid Tr(x\mathcal{O}) \subset \mathcal{O} \}$.

We have $\mathcal{O}^\vee \supset \mathcal{O}$ and $|\mathcal{O}^\vee / \mathcal{O}| = |\text{Discriminant}|$

<u>E.g.</u> $\mathcal{O} = \mathbb{Z}[i]$, $\mathcal{O}^\vee = \frac{1}{2}\mathcal{O}$.

<u>Exercise:</u> Discriminant of $\mathbb{Q}(\sqrt{\alpha}) = \begin{cases} \alpha & \text{if } \alpha = 1 \bmod 4 \\ 4\alpha & \text{otherwise.} \end{cases}$

Discriminant is a measure of how complicated a number field is.

(Note: we have no idea how many number fields there are, so having some measure of complexity is worthwhile.)

$\begin{array}{c} K \\ | \\ \mathbb{Q} \end{array}$ étale $\mathbb{Q}$-algebra $\rightsquigarrow$ $K \otimes_{\mathbb{Q}} \mathbb{R}$ étale $\mathbb{R}$-algebra $\cong \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}$

with $r_1 + 2r_2 = n$.

<u>Totally real</u> $\Leftrightarrow$ every embedding $K \hookrightarrow \mathbb{C}$ lands in $\mathbb{R}$ $\Leftrightarrow$ $r_1 = n$.

<u>Exercise:</u> Show that signature of $(Tr(\alpha_i, \alpha_j))$ is $(r_1 + r_2, r_2)$.

Totally real $\Leftrightarrow$ Trace form is positive definite.

Exercise: Let $K = \mathbb{Q}(e^{2\pi i/3})$, then $\mathcal{O} = \mathbb{Z}[e^{2\pi i/3}]$ and discriminant $= -3$.

Time for an analogy:

$$\left\{\begin{array}{l}\text{finite extensions } K \\ \text{of } \mathbb{C}(X) = \operatorname{Frac}\mathbb{C}[X]\end{array}\right\} \xleftarrow[\text{fields}]{\sim \text{ take function}} \left\{\begin{array}{c}C \text{ a smooth complex projective curve} \\ \downarrow \\ \mathbb{P}^1\mathbb{C}\end{array}\right\}$$

$\overset{\sim}{\leftrightarrow}$ Riemann surfaces w/ a map to $\mathbb{P}^1\mathbb{C}$.

(K is called a <u>function-field</u> over $\mathbb{C}$)

E.g.: $\mathbb{C}(X,Y)/(Y^2 - aX^3 - bX + c)$

$\uparrow$

$\mathbb{C}(X)$

How do we go back:

$$\begin{array}{ccccc} K & \supset & \mathcal{O} & \rightsquigarrow & \operatorname{Spec}\mathcal{O} \\ \downarrow & & \downarrow & & \downarrow \\ \mathbb{C}(X) & \supset & \mathbb{C}[X] & & \operatorname{Spec}\mathbb{C}[X] = \mathbb{A}^1 \end{array}$$

$\rightsquigarrow$ unique compactification.

Similarly we get:

$$\left\{\begin{array}{l}\text{finite extensions } K \\ \text{of } \mathbb{F}_p(X)\end{array}\right\} \overset{\sim}{\longleftrightarrow} \left\{\begin{array}{c}C \text{ a smooth projective curve } / \mathbb{F}_p \\ \downarrow \\ \mathbb{P}^1_{\mathbb{F}_p}\end{array}\right\}$$

we know rather well what a Riemann surface looks like.

<u>Very rough schematic of difficulty</u>: function fields over $\mathbb{C}$ $\ll$ function fields over $\mathbb{F}_p$ $\ll$ number fields

totally unknown

<u>See Weil:</u> Letter to sister Simone Weil.

<u>Example/exercise</u> (use of google allowed) Show that Fermat's last theorem is true in function fields. I.e. if $f, g, h \in k[X]$ are relatively prime and $f^n + g^n = h^n$, then $n = 2$.

Ideals:

Back to number fields: $\begin{array}{ccc} K & \supset & \mathcal{O} \\ \cup & & \cup \\ \mathbb{Q} & \supset & \mathbb{Z} \end{array}$

A fractional ideal I is a f.g. $\mathcal{O}$-submodule of K.

Given $I, J \rightsquigarrow$ product $IJ := \{ \sum \alpha_i \beta_j \mid \alpha_i \in I, \beta_j \in J \}$.

(remember product ~ union in algebraic geometry)

Remember $\mathcal{O}$ is a Dedekind domain,

(Krull-dim = 1) $\Rightarrow$ every prime ideal $\mathfrak{p} \neq 0$ is maximal

$\Rightarrow$ every fractional ideal has a unique factorisation

$$I = \prod \mathfrak{p}_i^{m_i} \quad \text{over prime ideals.}$$

$\mathcal{J}$ = group of non-zero fractional ideals under product

A fractional ideal is <u>principal</u> if it is of the form $\mathcal{O}x$ for $x \in K^\times$.

Fundamental exact sequence:

$$\begin{tikzcd}
 & & & \bigoplus_{\substack{\text{prime ideals} \\ \mathfrak{p} \neq 0}} \mathbb{Z}\mathfrak{p} & & \text{ideal class group} & \\
1 \arrow[r] & \mathcal{O}^\times \arrow[r] & K^\times \arrow[r] & P \arrow[r] & \mathcal{J} \arrow[r] \arrow[u, phantom, "\cup"] & Cl(\mathcal{O}) \arrow[r] & 0 \\
 & & & \text{principal ideals} \arrow[u] & \text{fractional ideals} \arrow[u] & \text{measures failure of } \mathcal{O} \text{ to be a PID.} \arrow[u] &
\end{tikzcd}$$

<u>Fundamental finiteness theorems:</u>

① $Cl(\mathcal{O})$ is a finite group,

② $\mathcal{O}^\times$ is f.g. of rank $r_1 + r_2 - 1$.

<u>Exercise:</u> Compute $\mathcal{O}^\times$ for quadratic extensions $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$.

(<u>Hint:</u> Pell's equation!)

Let us study the analogue of this for a smooth projective curve C.

Remember: prime ideal $\neq 0$ = maximal ideal = point of C

$$1 \to \mathbb{C}^\times \to K^\times \longrightarrow P \longrightarrow \bigoplus_{x \in C} \mathbb{Z}x \longrightarrow \mathrm{Pic}(C) \to 0$$

$K^\times$: K = function field of C

P: divisors of meromorphic functions

$\bigoplus_{x \in C} \mathbb{Z}x$: "divisors"

$\mathrm{Pic}(C)$: isomorphism classes of line bundles on C.

<u>Remark:</u> $\mathrm{Pic}(C) \xrightarrow{\sim} \mathbb{Z} \times \mathrm{Jac}(C)$

an abelian variety

Hence for complex curves, neither of the fundamental finiteness theorems hold.

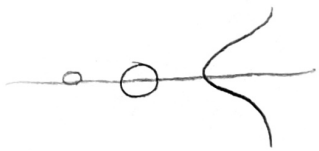
<u>Exercise*:</u> Show that if C is an affine curve over $\mathbb{F}_p$, then both finiteness theorems hold.

(if you know some algebraic geometry)

For K, $\mathcal{O}$ as above,

<u>Exercise:</u> Show that $K_0(\mathcal{O}) = \mathbb{Z} \oplus Cl(\mathcal{O})$.

(if you know K_0 and how to use it)



<u>Ramification</u>

$$\begin{array}{c} C \\ \downarrow f \\ \mathbb{P}^1\mathbb{C} \end{array}$$

e.g. $y^2 = f(x)$ for some polynomial $f(x)$ without repeated roots

Once we delete a finite set of points from $\mathbb{P}^1\mathbb{C}$ (the "discriminant" of f), then f is étale, and hence gives us a finite covering of $U \subset \mathbb{P}^1\mathbb{C}$.

Over finite fields, almost the same thing happens

$A = \mathbb{F}_p[x,y]/(y^2 = x^3+1)$ in char $p \neq 2, 3$

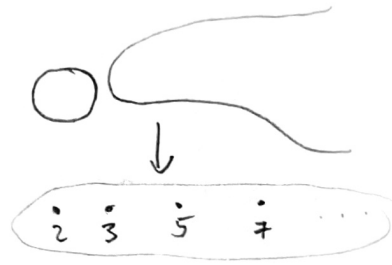
Again, this map is unramified away from a Zariski closed set.

Fibres of this map over a point $x = \lambda$ are

$$A \otimes_{x \mapsto \lambda} \mathbb{F}_p = \mathbb{F}_p[y]/(y^2 = \lambda^3+1) \cong \begin{cases} \mathbb{F}_p \times \mathbb{F}_p & \text{if } \lambda^3+1 \text{ is a residue mod } p \\ \mathbb{F}_{p^2} & \text{otherwise.} \end{cases}$$

Same picture is here for:

$$\begin{array}{c} \operatorname{Spec} \mathcal{O} \\ \downarrow \\ \operatorname{Spec} \mathbb{Z} \end{array}$$



$$\boxed{(p) = \prod_{i=1}^{g_p} \mathfrak{p}_i^{e_i}}$$

, for each such $\mathfrak{p}_i$, $\mathcal{O}/\mathfrak{p}_i$ is a finite extension of $\mathbb{F}_p$.

Write f_i for the degree of this extension.

$e_i =$ <u>ramification index</u>, $f_i =$ <u>inertia degree</u>

<u>Definition:</u>

1. (p) is unramified $\iff$ all $e_i = 1$, ramified otherwise.
2. (p) <u>splits completely</u> $\iff$ $f_i = e_i = 1$ for all i.
3. (p) is <u>inert</u> $\iff$ $g_p = 1$, $f_1 = 1$.

<u>Important exercise:</u> Show that $n = \sum e_i f_i$.

<u>Thm:</u> p is ramified in $\mathcal{O} \iff p \mid \operatorname{Disc}(K)$.

<u>Exercise:</u> Show that a finite-dim $\mathbb{F}_p$-algebra is étale $\iff$ its trace form is non-degenerate. Hence deduce theorem.

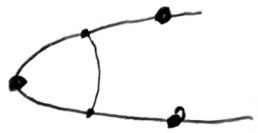
Example: $K = \mathbb{Q}(i)$, $\mathcal{O} = \mathbb{Z}[i]$.

$(1+i)^2 = 1 + 2i - 1 = 2i \Rightarrow (2) = (1+i)^2$, (2) is ramified.

Here $\operatorname{Disc} K = -4$, hence all other primes are unramified.

For all other p:

$$\mathcal{O}/(p) = \mathbb{Z}[x]/(p, x^2+1) = \mathbb{F}_p[x]/(x^2+1) = \begin{cases} \mathbb{F}_p \times \mathbb{F}_p & \text{if } \left(\frac{-1}{p}\right) = 1 \\ \mathbb{F}_p^2 & \text{if } \left(\frac{-1}{p}\right) = -1. \end{cases}$$



Hence p $\begin{cases} \text{splits completely} & \text{if } p \equiv 1 \bmod 4, \\ \text{is inert} & \text{if } p \equiv 3 \bmod 4. \end{cases}$

$\cancel{(2)\ (3)\ (5)\ \ldots}$

$\uparrow$ ramified

In general we can determine the splitting behaviour of most primes as follows:

Choose a primitive element $\theta \in K$, without loss of generality $\theta \in \mathcal{O}$.

Let $f(x)$ denote the minimal polynomial of θ.

Then $\mathbb{Z}[\theta] \subset \mathcal{O}$ will be finite index m.

For any $p \nmid m$ and coprime to the discriminant

$$\mathcal{O}/(p) \cong \mathbb{Z}[\theta]/(p) \cong \mathbb{Z}[x]/(p, f(x)) \cong \mathbb{F}_p[x]/(f(x)).$$

Hence, splitting behaviour of $f \bmod p$ determines splitting of (p) in $\mathcal{O}$.

Thus last week should have been discussing splitting of primes in a ring of integers.

Case of Galois extensions

$$\begin{array}{ccc} K & \supset & \mathcal{O} \\ | n & & | \\ \mathbb{Q} & \supset & \mathbb{Z} \end{array} \qquad G = \mathrm{Gal}(K/\mathbb{Q}) \circlearrowright \mathcal{O}$$

Frobenius: $\boxed{\text{If } (p) = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}, \text{ then } G \text{ acts transitively on the } \mathfrak{p}_i.}$

Hence all e_i (resp. f_i) are equal, denote them e_p, f_p.

$$\boxed{n = efg}$$

Fix $\mathfrak{p} = \mathfrak{p}_i$ and let $G_{\mathfrak{p}} :=$ stabiliser of $\mathfrak{p}$ ("decomposition group")

$|G/G_{\mathfrak{p}}| =$ primes over $(p) = g \Rightarrow |G_{\mathfrak{p}}| = ef$

$$1 \longrightarrow \underset{\substack{\uparrow \\ \text{inertia group}}}{\overset{\text{order } e}{I_{\mathfrak{p}}}} \longrightarrow \underset{\substack{\uparrow \\ \text{decomposition group}}}{\overset{\text{order } ef}{G_{\mathfrak{p}}}} \twoheadrightarrow \underset{\substack{\cong \\ \mathbb{F}_{p^f}}}{\overset{\text{order } f}{\mathrm{Aut}(\mathcal{O}/\mathfrak{p})}} \cong \mathbb{Z}/(f) \text{ generated by Frobenius}$$

If (p) is unramified, $e = 1$ and hence $I_{\mathfrak{p}}$ is trivial.

In this case we get $\mathrm{Frob}_{\mathfrak{p}} \in G_{\mathfrak{p}}$ mapping to the Frobenius.

Changing our choice of $\mathfrak{p}$ replaces $\mathrm{Frob}_{\mathfrak{p}}$ and $G_{\mathfrak{p}}$ by a conjugate. This explains rigourously our Frob_p from the last lecture.