WEEK 1.

p = prime

HENSEL (1897): "p-adic numbers" $\mathbb{Z}_p$.

Motivation: $f(x)$ polynomial with $\mathbb{Z}$-coefficients.

Suppose $r \in \mathbb{Z}$ is a root mod p:

$$f(r) \equiv 0 \pmod{p}$$

— Can one lift it to a root mod p^2?

Want an $s \in \mathbb{Z}$ s.t.

1) $s \equiv r \pmod{p}$ and

2) $f(s) \equiv 0 \pmod{p^2}$

Ex: Quadratic reciprocity → $x^2 \equiv a \,(p)$. Legendre symbol $\left(\frac{a}{r}\right)$. $(p \nmid a, p > 2)$

Taylor expansion: $f(x) = \sum_{n=0}^{N} c_n (x-r)^n$ with $c_n = \frac{f^{(n)}(r)}{n!} \in \mathbb{Z}$.

Insert $s = r + tp$ ← vary $t \in \mathbb{Z}$.

$$f(s) = \sum_{n=0}^{N} c_n (tp)^n = f(r) + f'(r)(tp) + \sum_{n=2}^{N} (\dots)$$

$$= f(r) + f'(r)(tp) + (tp)^2 g(t)$$

$$= mp + f'(r)(tp) + (tp)^2 g(t)$$

– Choose $t \in \mathbb{Z}$ for which

$$m + f'(r)t \equiv 0 \pmod{p}.$$

possible provided:

$$f'(r) \not\equiv 0 \pmod{p}$$

i.e., r is a simple root mod p.

(also shows the lift s unique mod p^2)

Same argument works for higher powers.

(n>0 fixed)

HENSEL'S LEMMA (v.1): Suppose

$$\begin{cases} f(r) \equiv 0 \pmod{p^n} & \text{and} \\ f'(r) \not\equiv 0 \pmod{p} \end{cases}$$

Then $\exists s \in \mathbb{Z}$ s.t. 1) $s \equiv r \pmod{p^n}$ and

2) $f(s) \equiv 0 \pmod{p^{n+1}}$

Furthermore, this s is unique mod p^{n+1}.

Thus, if r is a simple root mod p, it lifts uniquely up the tower:

$$\mathbb{Z}/p\mathbb{Z} \longleftarrow \mathbb{Z}/p^2\mathbb{Z} \longleftarrow \mathbb{Z}/p^3\mathbb{Z} \longleftarrow \cdots$$

$$[r] = [x_1] \longleftarrow [x_2] \longleftarrow [x_3]$$

where $f(x_n) \equiv 0 \pmod{p^n}$.

I.e., $[r]$ lifts uniquely to a root of f in

$$\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^n\mathbb{Z}$$

compatible sequences $([x_1], [x_2], [x_3] \ldots)$

- meaning: $x_{n+1} \equiv x_n \pmod{p^n}$.

Ring under componentwise add. & mult.

EXC: (1) $\mathbb{Z}_p$ integral domain ($\mathbb{Q}_p := \mathrm{Frac}(\mathbb{Z}_p)$)

Hint: Use "valuation" ($x \neq 0$)

$$v(x) = \max\{n \geq 0 : x_n \equiv 0 \ (p^n)\}$$

Check $v(xy) = v(x) + v(y)$. $x = (0000 \underbrace{***\ldots}_{\text{all nonzero}})$.

(2) $\mathbb{Z}_p$ local w. $m = (p) = p\mathbb{Z}_p$. (principal)

(and residue field $\mathbb{F}_p$)

Hint: Show $\mathbb{Z}_p \setminus m = \mathbb{Z}_p^\times$ by applying HENSEL to $cX - 1$ where $p \nmid c$.

Topology: $\mathbb{Z}_p \subseteq \prod_{n>0} \mathbb{Z}/p^n\mathbb{Z}$ compact and ~~Hausdorff~~ (Tychonoff).

neighborhood basis at 0:

$$p^n\mathbb{Z}_p = \{x : v(x) \geq n\}$$

↖ open balls for the metric

$$d(x,y) = p^{-v(x-y)} = |x-y|.$$

On $\mathbb{Z} \xrightarrow[\text{diag}]{} \mathbb{Z}_p$ this is the usual p-adic abs. value:

$(x], [x], [x], \ldots)$

$|x| = p^{-v}$ if $x = up^v$ with $p \nmid u$.

Note:

- $\mathbb{Z}_p$ is complete (Cauchy $\Rightarrow$ convergent); indeed a compact metric space.

extract Conv. subseq.

- $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ is dense.

(why? $x + p^n\mathbb{Z}_p$ contains an integer

$$x = ([x_1], \ldots, [x_n], \ldots)$$

$$= ([x_n], \ldots, [x_n], \ldots) \in x_n + p^n\mathbb{Z}_p)$$

Reformulation: $\mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}_p/p^n\mathbb{Z}_p$.

Conclude: $\mathbb{Z}_p$ is a complete local domain rng, $\mathrm{char}(\mathbb{Z}_p)=0$

w. residue field $\mathbb{F}_p$,

$$\mathbb{Z} \hookrightarrow \mathbb{Z}_p \text{ dense}$$

["p-adic completion"].

K = field.

An <u>absolute value</u> on K is $|\cdot| : K \longrightarrow [0,\infty)$ s.t.

(1) $|a| = 0 \iff a = 0$.

(2) $|ab| = |a| \cdot |b|$

(3) $|a+b| \leq |a| + |b|$ $\quad (\forall a,b \in K)$

Ex. ∘ The <u>trivial</u> one: $|a| = \begin{cases} 1 & a \neq 0 \\ 0 & a = 0 \end{cases}$.

— when K <u>finite</u> it's the <u>only</u> one ($a^n = 1$, $n = |K^\times|$ implies $|a| = 1$)

∘ the <u>ordinary</u> $|\cdot|_\infty$ on $\mathbb{R}$ and $\mathbb{C}$:

$$|z|_\infty = \sqrt{a^2+b^2}, \quad z = a+ib \in \mathbb{C}$$

$$|x|_\infty = \operatorname{sign}(x)\, x, \quad x \in \mathbb{R}.$$

∘ The p-<u>adic</u> $|\cdot|_p$ on $\mathbb{Q}$: $\forall\, x \neq 0$, write

$x = p^v \frac{a}{b}$ where $v \in \mathbb{Z}$ and $p \nmid ab$.

$$|x|_p = p^{-v}$$

sat. the "<u>strong triangle inequality</u>":

$$|x+y|_p \leq \max\{|x|_p, |y|_p\}$$

– Equivalently $v_p(x) := v$ defines a valuation, i.e.

(i) $v_p(x) = \infty \iff x = 0$

(ii) $v_p(xy) = v_p(x) + v_p(y)$

(iii) $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$

↑ why? May assume $x, y \in \mathbb{Z}$ by scaling.

$x = p^v a$, $y = p^w b$, $p \nmid ab$.

Suppose $v \leq w$. Then

$$x + y = p^v a + p^{w-v} p^v b$$

$$= p^v \underbrace{(a + p^{w-v} b)}_{\in \mathbb{Z} \text{ (may have "extra" factors } p)}$$

Shows $v_p(x+y) \geq v$. ✓

Note: Argument also shows that if $v < w$ then $v_p(x+y) = v$. I.e.,

$$|x+y|_p = \max\{|x|_p, |y|_p\}$$

provided $|x|_p \neq |y|_p$.

EXC ("PRODUCT FORMULA"): $\forall x \in \mathbb{Q}^\times$

$$\prod_{p \leq \infty} |x|_p = 1$$

(Hint: $\mathbb{Q}^\times$ generated by ± 1 and primes ℓ. Take $x = \ell$. $|\ell|_\infty = \ell$ and $|\ell|_p = \ldots$)

- $K = k(t) = \mathrm{Frac}\, k[t]$ (k finite field) $\quad \mathbb{P}^1$

$\mathfrak{p} \subseteq k[t]$ max ideal, $\mathfrak{p} = (p(t))$ ← irreducible, monic.

gives valuation

$v_{\mathfrak{p}}(f) =$ exponent of $\mathfrak{p}$ in factorization of $f(t)$

$|f|_{\mathfrak{p}} = q^{-v_{\mathfrak{p}}(f)}$ $\forall$ choice of $q > 1$. (usually $q = |k|$)

Moreover,

$\deg(f+g) \leq \max\{\deg f, \deg g\}$

so $v_\infty = -\deg$ is another valuation on K.

$|f|_\infty = q^{\deg(f)}$

— all sat. strong triangle inequality.

(product formula?)

Proposition $|\cdot|$ on K sat. strong triangle inequality iff $|\cdot|$ is bounded on $\mathbb{Z} \cdot 1_K$.

[If so we say $|\cdot|$ is non-archimedean.]

PROOF. $\Downarrow$: $|m \cdot 1_K| = |\underbrace{1 + \cdots + 1}_{m}| \overset{\max}{\leq} |1| = \boxed{1}$

(for $m > 0$)

$\Uparrow$: Suppose $|m \cdot 1_K| \leq N$, $\forall m \in \mathbb{Z}$.

— Then, for all $n > 0$, and $x, y \in K$,

$$|x+y|^n \overset{(2)}{=} \left| \sum_{r=0}^{n} \binom{n}{r} x^r y^{n-r} \right|$$

$$\overset{(3)}{\leq} \sum_{r=0}^{n} \underbrace{\left|\binom{n}{r}\right|}_{\leq N} \cdot \underbrace{|x|^r \cdot |y|^{n-r}}_{\leq \max\{|x|,|y|\}^n}$$

$$\leq N(n+1) \cdot \max\{|x|,|y|\}^n$$

n^{th} roots:

$$|x+y| \leq N^{1/n} \cdot (n+1)^{1/n} \cdot \max\{|x|,|y|\}$$

Let $n \to \infty$. $\quad (n+1)^{1/n} \to 1$ $\quad \square$

[Corollary If $\mathrm{char}(K) > 0$ then every $|\cdot|$ on K is non-archimedean. (since $\mathbb{Z} \cdot 1_K$ finite)

★ Observation: (cf. $|\cdot|_p$ discussion above) If $|\cdot|$ is non-archimedean,

$$|x+y| = \max\{|x|,|y|\}$$

provided $|x| \neq |y|$.

Why? Suppose $|x| > |y|$. Then:

$$|x+y| \leq \max\{|x|, |y|\} = |x|.$$

must be equality — otherwise

$$|x| = |x+y-y| \leq \max\{|x+y|, |y|\} < |x|.$$

(contradiction) both are $< |x|$.

Exc (1) If $|\cdot|$ is an abs. value, so is $|\cdot|^c$ for $0 < c \leq 1$.

show:

$$(|x|+|y|)^c \leq |x|^c + |y|^c \quad \leftarrow \text{FALSE } c=2.$$

(2) $|\cdot|$ is non-archimedean $\iff$ $|\cdot|^c$ abs. value for all $c > 0$.

($\Rightarrow$ easy. $\Leftarrow$:

$$|m \cdot 1_K|^c \leq \underbrace{|1_K|^c + \cdots + |1_K|^c}_{m} = m$$

Take $(\cdot)^{1/c}$ and let $c \to \infty$)

Exc Given $|\cdot|$ non-archimedean, $x_1, \ldots, x_n \in K$.
Suppose $\max\{|x_1|, \ldots, |x_n|\}$ is achieved once (some $|x_i| > |x_j|$ for all $j \neq i$)
Then $\max\{\cdots\} = |x_1 + \cdots + x_n|$.

Hint: $i = 1$. Then $|x_1| > \max\{|x_2|, \ldots, |x_n|\}$. So:

$$|x_1 + (x_2 + \cdots + x_n)| = \max\{|x_1|, |x_2 + \cdots + x_n|\} = |x_1|. \quad \checkmark$$

($=$: $n=2$ case.)

K = field w. absolute value $|\cdot|$.

Metric: $d(x,y) = |x-y|$.

- hence topology w. basis of open balls $B_r(x) = \{y : |x-y| < r\}$.

Note: $|\cdot|_{triv}$ gives the discrete top.: $B_r(x) = \{x\}$ for $r \leq 1$.

- Thus K becomes a topological field ($+$ and $\cdot$ cont.) and $|\cdot| : K \to [0,\infty)$ continuous; indeed

$$\big|\,|x| - |y|\,\big| \leq |x-y| \qquad \text{(exc.)}$$

Def. $|\cdot|_1$ and $|\cdot|_2$ on K are equivalent if they def. the same top.

Ex. $|\cdot|_\infty$ and $|\cdot|_p$ on $\mathbb{Q}$ are inequivalent:

$p^n \to 0$ as $n \to \infty$ rel. $|\cdot|_p$, not $|\cdot|_\infty$.

- Similarly $|\cdot|_p$ and $|\cdot|_q$ are inequivalent for $p \neq q$: $|p^n|_q = 1$.

"Ostrowski's Thm": (LATER)
Every non-triv. $|\cdot|$ on $\mathbb{Q}$ is $\sim$ to either $|\cdot|_\infty$ or a unique $|\cdot|_p$.

– Extends to number fields $K/\mathbb{Q}$:

1) Every max $\mathfrak{p} \subseteq \mathcal{O}_K$ gives non-arch. $|x|_{\mathfrak{p}} = N(\mathfrak{p})^{-v_{\mathfrak{p}}(x)}$.

2) Every embedding $\tau : K \to \mathbb{C}$ gives $|x|_\tau = |\tau(x)|_\infty$.

(obviously $|\cdot|_\tau = |\cdot|_{\overline{\tau}}$)

FACT: Real embeddings give ineq. $|\cdot|_\tau$.

$K = \mathbb{Q}(\sqrt{2})$ has two: ↖ "θ" $\theta^2 = 2$.

$$\begin{cases} \tau(\theta) = \sqrt{2} \\ \sigma(\theta) = -\sqrt{2}. \end{cases}$$

$$|(1+\theta)^n|_\tau = |(1+\sqrt{2})^n|_\infty = (1+\sqrt{2})^n \longrightarrow \infty$$

$$|(1+\theta)^n|_\sigma = |(1-\sqrt{2})^n|_\infty = (\sqrt{2}-1)^n \longrightarrow 0.$$

★ REMARK: $|\cdot| \sim |\cdot|_{triv} \overset{\text{obv.}}{\Longrightarrow} |\cdot| = |\cdot|_{triv}$.

(i.e., $|\cdot|$ gives the discrete top.)

($x \neq 0$. Show $|x| = 1$.
If $|x| < 1$, $x^n \to 0$ in disc. top.
i.e., $x^n = 0$, $n >> 0$.
$\Rightarrow x = 0$.
If $|x| > 1$, consider x^{-1})

Prop. $|\cdot|_1$ and $|\cdot|_2$ non-triv. abs. values on K. T.F.A.E.:

(1) $|\cdot|_1 \sim |\cdot|_2$ (define same topology)

(2) $|\cdot|_2 = |\cdot|_1^c$ for some $c>0$.

(3) $|x|_1<1$ implies $|x|_2<1$

(Can add: They have same open unit ball at 0)

PROOF: (2) $\Rightarrow$ (1): Same balls ($r \rightsquigarrow r^c$).

(1) $\Rightarrow$ (3): $|x|_1<1$ implies $x^n \to 0$ rel. $|\cdot|_1$, thus rel. $|\cdot|_2$. I.e., $|x|_2<1$.

(3) $\Rightarrow$ (2): Pick $y \in K$ with $|y|_1>1$. ← non-triv.
Then also $|y|_2>1$
(apply (3) to y^{-1})

* CLAIM: $c = \dfrac{\ln|y|_2}{\ln|y|_1} > 0$ works in (2).

note: $|y|_2 = |y|_1^c$ (A)

I.e.,
$$|x|_2 = |x|_1^c \text{ for all } x.$$

Fix an $x \neq 0$. Put $b = \dfrac{\ln|x|_1}{\ln|y|_1} \in \mathbb{R}$

— Will show: $|x|_2 = |y|_2^b$.

note: $|x|_1 = |y|_1^b$ (B)

(sufficient since then
$|x|_2 = |y|_2^b = |y|_1^{bc} = |x|_1^c$:)
(A) (B)

– First, choose any $\frac{m}{n} > b$. Then,

$$|x|_1 \underset{(B)}{=} |y|_1^b < |y|_1^{\frac{m}{n}} \Rightarrow \left|\frac{x^n}{y^m}\right|_1 < 1 \overset{(3)}{\Rightarrow} \left|\frac{x^n}{y^m}\right|_2 < 1$$

meaning $|x|_2 < |y|_2^{\frac{m}{n}}$. Letting $\frac{m}{n} \searrow b$ yields $|x|_2 \leq |y|_2^b$.

– Second, same argument with $\frac{m}{n} \nearrow b$ yields $|x|_2 \geq |y|_2^b$. $\square$

Ostrowski ($K = \mathbb{Q}$): Every non-triv. $|\cdot|$ is equivalent to either $|\cdot|_\infty$ or $|\cdot|_p$ for a unique p. / done.

PROOF: (1) First suppose $|\cdot|$ non-archimedean (i.e., $|m| \leq 1 \ \forall m \in \mathbb{Z}$)

– Pick an $n \in \mathbb{N}$ with

$$|n| < 1.$$

↖ non-trivial.

exists? Othw. $|x| = 1 \ \forall x \in \mathbb{Q}^\times$.

Assume n is the smallest such. (well-ordering)

This n must be a prime:

$n = ab$

$1 > |n| = |a| \cdot |b|$

↖ ↗

each ≤ 1; cannot both be 1.

If $|a| < 1$, $a = n$ by minimality.

etc.

Rename it p; $|p| < 1$.

CLAIM: $|\cdot| \sim |\cdot|_p$.

*) prelim. obs.:

$a \in \mathbb{Z}$, $|a| < 1 \Rightarrow p \mid a$.

[indeed $a = mp + r$, $0 \leq r < p$.

so, $|r| \leq \max\{|a|, |mp|\} < 1$. Minimality of p gives $r = 0$].

Let $a \in \mathbb{Z}$ be nonzero.

$$a = p^{v_p(a)} u \quad \text{where } p \nmid u.$$

Note: $|u| = 1$.

(know $|u| \leq 1$ and cannot be < 1 by obs. (*))