4.1. Given an ~~[illegible]~~ ext L/K, basis $\alpha_1, \dots, \alpha_n$.

$$\mathrm{Disc}(\alpha_1, \dots, \alpha_n) := \det \begin{bmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & & \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_n) \end{bmatrix}^2$$

$$= \det(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)).$$

Also, $\mathrm{Disc}(1, \theta, \theta^2, \theta^3, \dots \theta^{n-1}) = \prod_{i<j} (\theta_i - \theta_j)^2$.

Facts. $^{\circledast}$ Change of basis. If $\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = A \cdot \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix}$

then $\mathrm{Disc}(\alpha_1, \dots, \alpha_n) = \det(A)^2 \cdot \mathrm{Disc}(\beta_1 \cdots \beta_n)$.

A fact about bilinear forms, of which $\begin{array}{l} L \times L \longrightarrow K \\ (\alpha, \beta) \to \mathrm{Tr}_{L/K}(\alpha\beta). \end{array}$

$\circledast$ If $L = \mathbb{Q}(\alpha)$, and $f(x)$ is the min poly of α, then

$$D(1, \alpha, \dots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{L/\mathbb{Q}} \overbrace{f'}^{\text{usual derivative}}(\alpha).$$

(calculus. check it.)
(Thm 44 in MF)

Prop. Given the usual setup

$$\begin{array}{ccc} L & — & B \\ | & & \\ K & — & A \end{array} \quad \left(\text{if you like: } \begin{array}{ccc} L & — & \mathcal{O}_K \\ | & & \\ \mathbb{Q} & — & \mathbb{Z} \end{array}\right)$$

and $\alpha_1, \dots \alpha_n$ a basis of L/K contained in B,

then write $d = \mathrm{Disc}(\alpha_1, \dots, \alpha_n)$.

We have $dB \subseteq A\alpha_1 + A\alpha_2 + \dots + A\alpha_n$.

4.2. Proof. This uses our linear algebra trick again.

If $\beta = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n \in B$ (which it is for all

we have $\underbrace{\mathrm{Tr}_{L/K}(\alpha_i \beta)} = \sum_j \mathrm{Tr}_{L/K}(\alpha_i\alpha_j)\cdot a_j$

Note: $\alpha_i\beta \in B$, so its trace is in A.

$$= \left[(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)) \right] \begin{bmatrix} a_1 \\ \vdots \\ a_j \end{bmatrix}$$

$$\left[\mathrm{Tr}_{L/K}(\alpha_i\alpha_j) \right]^* \left[\mathrm{Tr}_{L/K}(\alpha_i\alpha_j) \right] \begin{bmatrix} a_1 \\ \vdots \\ a_j \end{bmatrix}$$

adjoint

$$= d \cdot \begin{bmatrix} a_1 \\ \vdots \\ a_j \end{bmatrix}.$$

This has entries in A,
because the adjoint matrix
and $\left[\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)\right]\begin{bmatrix} a_1 \\ \vdots \\ a_j \end{bmatrix}$ does.

And so if $\beta = a_1\alpha_1 + \cdots + a_n\alpha_n \in B$,
then $d\cdot\beta = (da_1)\alpha_1 + \cdots + (da_n)\alpha_n$
$\in A\alpha_1 + \cdots + A\alpha_n$.

(IMHO, a little bit of a weird proof.)

Now: Back to the punchline.

Theorem. Let $K/\mathbb{Q}$ be a number field.
Then an integral basis exists for K.

(Can argue
$$\begin{array}{ccc} L & - & B \\ | & & \\ K & - & A \end{array}$$
if A is a PID.)

Proof. Choose a basis $x_1, \dots, x_n$ of K.
For some constant c, $cx_1, \dots, cx_n$ are all in $\mathcal{O}_K$.

So $\mathcal{O}_K \supseteq \mathbb{Z}\cdot(cx_1) + \cdots + \mathbb{Z}(cx_n)$.

By previous, $d\cdot\mathcal{O}_K \subseteq \mathbb{Z}(cx_1) + \cdots + \mathbb{Z}(cx_n)$.

By structure thm for abelian groups (f.g. modules / PIDs)
$\mathcal{O}_K$ is a free $\mathbb{Z}$-module.

Def. If $K/\mathbb{Q}$ is a number field, let $a_1, \dots, a_n$ be an integral basis.

Then $\text{Disc}(K) := \text{Disc}(a_1, \dots, a_n)$.

Note. For an extension L/K we have a "relative discriminant" $\text{Disc}_{L/K}$ (or $\Delta_{L/K}$). It is an ideal of K.

But L/K may not have an integral basis.

Def. is more complicated.

Example. Let θ be a root of $x^3 + 2x + 1$.

Compute $\text{Disc}(\mathbb{Q}(\theta))$.

Two steps.

(1) Hope that $\mathbb{Q}(\theta)$ has an integral basis, i.e. if $K = \mathbb{Q}(\theta)$, then $\mathcal{O}_K = \mathbb{Z}[\theta]$.

Compute $\text{Disc}(\mathbb{Z}[\theta]/\mathbb{Z})$.

(2) Check that we got lucky.

There are multiple ways to do (1).

(a) $$\text{Disc}\ \mathbb{Z}[\theta]/\mathbb{Z} = \det \begin{bmatrix} \text{Tr}(1) & \text{Tr}(\theta) & \text{Tr}(\theta^2) \\ \text{Tr}(\theta) & \text{Tr}(\theta^2) & \text{Tr}(\theta^3) \\ \text{Tr}(\theta^2) & \text{Tr}(\theta^3) & \text{Tr}(\theta^4) \end{bmatrix}.$$

Now, can replace θ^3 with $-2\theta - 1$, etc.

Computing the traces: can do in terms of conjugates

($\text{Tr}\ \theta^2$ is not obvious from inspection)

or write out as an endomorphism: mul by θ^2:

$1 \to \theta^2$

$\theta \to \theta^3 = -2\theta - 1$

$\theta^2 \to \theta^4 = -2\theta^2 - \cancel{\theta}.$

4.4. This means, mult. by θ^2 has matrix

$$\begin{bmatrix} 0 & -1 & 0 \\ 0 & -2 & -1 \\ 1 & 0 & -2 \end{bmatrix}$$ which has trace -4.

So: $Tr(1) = 3$.
$Tr(\theta) = 0$.
$Tr(\theta^2) = -4$
$Tr(\theta^3) = Tr(-2\theta - 1) = -3$
$Tr(\theta^4) = Tr(-2\theta^2 - \theta) = 8$.

and $\det \begin{bmatrix} 3 & 0 & -4 \\ 0 & -4 & -3 \\ -4 & -3 & 8 \end{bmatrix} = 3(-32-9) - 4(0-16)$
$= -123 + 64 = -59$.

(b) we have $\text{Disc } \mathbb{Z}[\varphi]/\mathbb{Z} = -N_{\mathbb{Q}(\varphi)/\mathbb{Q}}(3\varphi^2+2)$.
Let $\gamma = 3\varphi^2 + 2$. Write out min poly.
$\gamma^3 = \ldots$ figure out what to cancel.

(c) See also Milne, pp. 38-39.
(d) The disc is $[(\theta-\theta')(\theta-\theta'')(\theta'-\theta'')]^2$. Multiply out. Get a symmetric polynomial in coeffs.
Now certainly $\mathbb{Z}[\theta] \subseteq \mathcal{O}_K$, and we have

$$\text{Disc}(\mathcal{O}_K/\mathbb{Z}) = \frac{\text{Disc}(\mathbb{Z}[\theta]/\mathbb{Z})}{[\mathcal{O}_K : \mathbb{Z}[\theta]]^2}.$$

and, $\text{Disc}(\mathcal{O}_K/\mathbb{Z})$ must be an integer.
59 does not have any square factors, so we must be done.

Ex<u>ample</u>. Do the same for $x^3 - x - 4$.
$\text{Disc}(1, \theta, \theta^2)$ is -428.
Divisible by 4, so look for something that doubles into this.
In fact $\frac{\theta+\theta^3}{2} \in \mathcal{O}_K$.

4.5.

Proposition. (M. 2.40)

* The sign of $\mathrm{Disc}(K/\mathbb{Q})$ is $(-1)^s$,

  $2s$ is # of complex embeddings $K \hookrightarrow \mathbb{C}$.

* (Stick.) $\mathrm{Disc}(\mathcal{O}_K/\mathbb{Z})$ is $\equiv 0, 1 \pmod 4$.

  Read it in Milne. (somewhat Galois theoretic)

Proof of (1).

Let $K = \mathbb{Q}(\alpha)$.

$\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_r$ real conjugates

$\alpha_{r+1}, \overline{\alpha_{r+1}}, \ldots, \alpha_{r+s}, \overline{\alpha_{r+s}}$ complex conjugates.

Then ~~$\mathrm{Disc}(\alpha_1, \ldots, \alpha_{r+s})$~~

$$\mathrm{Disc}(1, \alpha, \ldots, \alpha^{n-1}) = \prod (\alpha - \alpha')^2 \qquad n = r + 2s$$

Most everything is a square of a real number, or its complex conjugate also appears.

Only exception:

$$\prod_{i=1}^{s} \left(\alpha_{r+i} - \overline{\alpha_{r+i}}\right)^2$$

$$= \prod_{i=1}^{s} (\text{something negative}).$$

[If time: riff on open problems]

5.1.

Definition. An integral domain A is a Dedekind domain if

(1) it is noetherian (any ideal is finitely generated)

(2) it is integrally closed (in its field of fractions)

(3) every prime ideal $\neq (0)$ is maximal.

Ex. If A is a PID then A is Dedekind.

(1) is trivial.

(2) : PIDs are UFDs which are integrally closed.

(3) Every prime ideal $\neq (0)$ is maximal. (Easy to check)

Ex. $\mathbb{C}[x, y]$ is not a Dedekind domain.

(x) is a nonmaximal prime.

Thm. Let A be a Dedekind domain with f.f. K. L/K finite separable, B the integral closure of A in L. Then B is Dedekind.

Proof.

(1) B is noetherian: MF, Thm. 66 (in case we care about)

(2) B is an integral closure.

(3) Let $\mathfrak{p} \subset B$ be a nonzero prime.

We know $\mathfrak{p}$ is maximal $\longleftrightarrow$ $B/\mathfrak{p}$ is a field

(also recall: $\mathfrak{p}$ is prime $\longleftrightarrow$ $B/\mathfrak{p}$ is a domain)

Claim. Write $\mathfrak{m} = A \cap \mathfrak{p}$. Then $\mathfrak{m}$ is ~~maximal~~ nonzero.

Proof. If $\beta \in \mathfrak{p}$, it is integral over A.

We have $\beta^n + a_1\beta^{n-1} + a_2\beta^{n-2} + \cdots + a_n = 0$ $(a_i \in A)$ of min degree.

5.2. $a_n = -(\beta^n + a_1\beta^{n-1} + \cdots + a_n\beta)$ which is in ~~[illegible]~~ $A \cap \mathfrak{p}$!

Now $\underline{m}$ is prime in A (since $\mathfrak{p}$ is), so $\underline{m}$ is maximal in A, so $A/\underline{m}$ is a field.

Want to show, $B/\mathfrak{p}$ is a field.

$\mathfrak{p}$ is a prime, so $B/\mathfrak{p}$ is a domain.

Consider the map

$$A/\underline{m} \longrightarrow B/\mathfrak{p}$$

$$a + \underline{m} \longrightarrow b + \mathfrak{p} \quad (\underline{\text{injective}})$$

Since B/A is integral, $B/\mathfrak{p}$ is algebraic over $A/\underline{m}$.

The following lemma will finish the proof.

<u>Lemma</u>. A domain B containing a field k and algebraic over k is a field.

<u>Proof</u>. Given $\beta \in B$. Then $k[\beta]$ is a f.d. vector space over k.

The map
$$k[\beta] \longrightarrow k[\beta]$$
$$x \longrightarrow \beta x$$
is an isomorphism of <u>vector</u> <u>spaces</u>.

So β is invertible, so $k[\beta]$ is a field, so done.

<u>Unique factorization</u>.

Rings of integers are not in general UFD's.

<u>Ex</u>. $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$.
$$\underset{\substack{\uparrow \\ \text{norm} \\ 4}}{2} \cdot \underset{\substack{\uparrow \\ \text{norm} \\ 9}}{3} = \underset{\substack{\uparrow \\ \text{norm } 6}}{(1+\sqrt{-5})}\underset{\substack{\uparrow \\ \text{norm } 6.}}{(1-\sqrt{-5})}.$$

But there is no element of norm 2, because $a^2 + 5b^2 = 2$ has no solutions.

5.3. Note. Prime $\neq$ irreducible!

All elements above are irreducible, but

$$2 \mid (1+\sqrt{-5})(1-\sqrt{-5})$$

$$2 \nmid 1+\sqrt{-5}$$

$$2 \nmid 1-\sqrt{-5} \quad \text{so } 2 \text{ is not prime.}$$

<u>Theorem</u>. Let B be a Dedekind domain. Then any ideal of B can be written uniquely as a product of prime ideals.

<u>Proofs</u>. MF, Thm. 75; Milne, Thm. 3.7.

Ex<u>ample</u>. We have, in $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$,

$$(6) = (2)\cdot(3) = (1+\sqrt{-5})\cdot(1-\sqrt{-5})$$

must have further factorization.

(Implicitly using: $N(a)$ = product of conjugates
$N((a)) = |\mathcal{O}_K/(a)|$
Norms are multiplicative)

We have prime ideals $(2, 1+\sqrt{-5})$
$(3, 1+\sqrt{-5})$

and $(2) = (2, 1+\sqrt{-5})\cdot(2, 1-\sqrt{5})$.
(Note: These ideals are ~~not~~ equal.

$(3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$ (<u>not</u> equal)

$$(1+\sqrt{-5}) = (2, 1+\sqrt{-5})(3, 1+\sqrt{-5})$$

$$(1-\sqrt{-5}) = (2, 1-\sqrt{-5})(3, 1-\sqrt{-5}).$$

E<u>x</u>. Check all of the above.

<u>Thm</u>. Any ~~prime~~ ideal can be generated by two elements, one of which is in $\mathbb{Z}$. (See p. 73 of MF, will return!!)

5.4. **Theorem.** (Chinese Remainder)

Given a ring R, and ideals $\mathfrak{a}_1 \dots \mathfrak{a}_n$ with $\mathfrak{a}_i + \mathfrak{a}_j = R$ if $i \neq j$.

Then,
$$R/\cap \mathfrak{a}_i \cong \oplus R/\mathfrak{a}_i.$$

Proof. Consider the homomorphism
$$R \longrightarrow \oplus R/\mathfrak{a}_i$$
$$r \longrightarrow (r+\mathfrak{a}_1, \dots, r+\mathfrak{a}_n).$$
Visibly, the kernel is $\cap \mathfrak{a}_i$. So prove surjective.

Surjectivity for $n=2$.
We can write $1 = a_1 + a_2$ where $a_1 \in \mathfrak{a}_1$, $a_2 \in \mathfrak{a}_2$,

and so $a_1 \equiv 1 \pmod{\mathfrak{a}_2}$, $\equiv 0 \pmod{\mathfrak{a}_1}$ and vice versa
$$xa_1 + ya_2 \longrightarrow (ya_2, xa_1)$$
$$= (y, x) \text{ in } R/\mathfrak{a}_1 \oplus R/\mathfrak{a}_2$$
choose x, y anything you want.

$n > 2$. Similar story.

~~Write~~ Find $b_{1,2} \equiv 1 \pmod{\mathfrak{a}_1}$ and $\equiv 0 \pmod{\mathfrak{a}_2}$

$b_{1,3} \equiv 1 \pmod{\mathfrak{a}_1}$ and $\equiv 0 \pmod{\mathfrak{a}_3}$

$\vdots$

$b_{1,n} \equiv 1 \pmod{\mathfrak{a}_1}$ and $\equiv 0 \pmod{\mathfrak{a}_n}$

$$b_1 = b_{1,2} \cdot b_{1,3} \cdot \dots \cdot b_{1,n} \equiv 1 \pmod{\mathfrak{a}_1}$$
$$\equiv 0 \pmod{\mathfrak{a}_i} \text{ for } i \neq 1.$$

Then $b_1 \longrightarrow (1, 0, 0, \dots, 0)$.
Similarly can find elts mapping to $(0, 1, 0, 0, \dots, 0)$ etc.
and these generate $\oplus R/\mathfrak{a}_i$. ∎

5.5.

Prop. In a Dedekind domain R, if $\underline{a}_1 + \underline{a}_2 = R$ then $\underline{a}_1$ and $\underline{a}_2$ are coprime.

This is easy. If $\underline{a}_1 = \underline{p}\,\underline{b}_1$ for some $\underline{p}, \underline{b}_1$,

$\underline{a}_2 = \underline{p}\,\underline{b}_2$

then $\underline{a}_1 + \underline{a}_2 = \underline{p}\,\underline{b}_1 + \underline{p}\,\underline{b}_2 \subseteq \underline{p}$.

It goes the other way too.

If $\underline{a}_1 + \underline{a}_2 = \underline{a} < R$,

then $\underline{a}_1 \subseteq \underline{a}$, $\underline{a}_2 \subseteq \underline{a}$ and so $\underline{a}_1 = \underline{a} \cdot \underline{b}_1$, $\underline{a}_2 = \underline{a} \cdot \underline{b}_2$ for some $\underline{b}_1, \underline{b}_2$.

(MF, Prop. 69. containment $\longleftrightarrow$ divisibility.)

Prop. If $\underline{a}_1 \ldots \underline{a}_n$ are pairwise coprime ideals, then

$$\underline{a}_1 \cdot \underline{a}_2 \cdots \underline{a}_n = \underline{a}_1 \cap \cdots \cap \underline{a}_n .$$

$\subseteq$ is obvious.

$\supseteq$: Do a simple induction, or :
if $a \in \underline{a}_1 \cap \cdots \cap \underline{a}_n$, then for each i, $\underline{a}_i \mid (a)$.
Since the i's are coprime, $\underline{a}_1 \cdots \underline{a}_n \mid (a)$.
i.e., $a \in \underline{a}_1 \cdots \underline{a}_n$.

So: CRT restated.

In a Dedekind domain, if $\underline{a} = \prod \underline{a}_i$ with the $\underline{a}_i$ coprime,

$$R/\underline{a} \cong \bigoplus_i R/\underline{a}_i .$$ (usual CRT!)

6.1. The p-adic numbers.

(1) As a completion of $\mathbb{Q}$

(2) As an inverse limit of $\mathbb{Z}/p^n$

(3) As formal power series $a_0 + a_1 p + a_2 p^2 + \cdots$

Motivation. (K. Hensel, 1897)

Instead of $\mathbb{Z}$ and $\mathbb{Q}$, think of $\mathbb{C}[x]$ and $\mathbb{C}(x)$.

The primes of $\mathbb{C}[x]$ are $(x-a)$ for $a \in \mathbb{C}$ (and (0))

and we have a correspondence

$$\text{primes of } \mathbb{C}[x] \longleftrightarrow \mathbb{C}.$$

(and 0)

Pick any $a \in \mathbb{C}$. We can write any poly. $g(x) \in \mathbb{C}[x]$ as $a_0 + a_1(x-a) + a_2(x-a)^2 + \cdots + a_n(x-a)^n$.

Complex analysis theorem. Any holomorphic function $f(x)$ has a power series representation

$$f(x) = a_0 + a_1(x-a) + a_2(x-a)^2 + a_3(x-a)^3 + \cdots$$

In general, if $f(x)$ is meromorphic in a nbd. of a, can write

$$f(x) = a_{-n}(x-a)^{-n} + a_{-n+1}(x-a)^{-n+1} + \cdots + a_0 + a_1(x-a) + \cdots$$

For example, suppose $f(x) = \dfrac{P(x)}{Q(x)}$ is a rational function.

Then for any a, we can write $f(x)$ as above.

Here n will be the order of the pole at a.

6.2.

This is like writing integers in base p.

e.g. $p = 7$. $\quad 100 = 2 \cdot 7^2 + 0 \cdot 7^1 + 2 \cdot 7^0$.

Can we write $\frac{1}{5}$ as an integer in base 7?

Ex. Find the Taylor series expansion of $\frac{1}{x+1}$ around $x = 0$.

Solution.

Do calculus, or let the answer be $a_0 + a_1 x + a_2 x^2 + \cdots$

$$(a_0 + a_1 x + a_2 x^2 + \cdots) \times (x+1) = 1 = 1 + 0x + 0x^2 + \cdots$$

Solve for a_0: $\quad a_0 = 1$.

$a_0 + a_1 = 0$. $\quad$ So $a_1 = -1$.

$a_2 + a_1 = 0$. $\quad$ So $a_2 = 1$.

Keep solving one coeff. at a time.

Ex. Write $\frac{1}{5}$ as a "7-adic integer"

$$a_0 + a_1 \cdot 7 + a_2 \cdot 7^2 + a_3 \cdot 7^3 + \cdots$$

Solve in the same way. A little different because of carrying.

$$5 \cdot (a_0 + a_1 \cdot 7 + a_2 \cdot 7^2 + a_3 \cdot 7^3 + \cdots) = 1 + 0 \cdot 7 + 0 \cdot 7^2 + \cdots$$

$5a_0 = 1$, so $a_0 \equiv 3 \pmod 7$.

$5(a_0 + 7a_1) \equiv 1 \pmod{49}$.

$35a_1 \equiv 1 - 15 \pmod{49}$

$35a_1 \equiv 35 \pmod{49}$

$a_1 \equiv 1 \quad (\text{mod } 49 \text{ or mod } 7)$.

One more.

$$5(3+7+49a_2) \equiv 1 \mod 343.$$

$$5 \cdot 49 a_2 \equiv 1 - 50 \mod 343.$$

$$5 \cdot 49 a_2 \equiv -49 \mod 343$$

$$5a_2 \equiv -1 \mod 7$$

$$a_2 \equiv -1 \cdot \overline{5} \mod 7$$

$$\equiv -1 \cdot 3 \mod 7$$

$$= -3 \pmod 7.$$

So $\frac{1}{5} = 3 + 1 \cdot 7 + \underbrace{(-3)}_{\text{or, write } 4} \cdot 7^2 + \cdots$

Exercise. (1) Continue this process through a_6.

(2) Prove that it can be continued indefinitely.

(3) Prove it works for any $\frac{a}{b}$ with $7 \nmid b$.

(4) If we replace 7 with p, prove it works for any $\frac{a}{b}$ with $p \nmid b$.

Ex. (won't work) Write $\frac{1}{7}$ as a 7-adic integer.

Proof. Suppose we can write $\frac{1}{7} = a_0 + a_1 \cdot 7 + a_2 \cdot 7^2 + \cdots$

Then $1 = 7(a_0 + a_1 \cdot 7 + a_2 \cdot 7^2 + \cdots)$

as before, solve mod 7, mod 7^2, mod 7^3, etc.

But we can't solve mod 7.

First step would be, $1 \equiv 7a_0 \mod 7$

$1 \cdot \overline{7} \equiv a_0 \mod 7$

but we cannot invert 7 mod 7.

6.4. Definition. The p-adic integers $\mathbb{Z}_p$ are the formal infinite series

$$a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots$$

where $0 \le a_i < p$ for all i.

These form a ring. But careful. You have to carry.

e.g. Let $p = 5$.

Then $(2) + (3 + 1 \cdot 5)$

$= (2 + 3) + 1 \cdot 5$

$= 5 + 1 \cdot 5 = 2 \cdot 5$.

Note. This is just usual damn arithmetic.

Ex. Again $p = 5$.

Compute $2 \times (2 + 2 \cdot 5 + 2 \cdot 5^2 + 2 \cdot 5^3 + \cdots) + 1$.

Answer. It's $(4 + 4 \cdot 5 + 4 \cdot 5^2 + 4 \cdot 5^3 + \cdots) + 1$

i.e.

$$\begin{array}{r} \cdots \overset{1}{4}\overset{1}{4}\overset{1}{4}4 \\ + \qquad\quad 1 \\ \hline \cdots 0000 \end{array} = 0.$$

write mod p, with decimals to the left.

So $\cdots 222 = -\frac{1}{2}$.

You can figure out how to multiply. But we'll be more formal anyway.

Def. The p-adic numbers $\mathbb{Q}_p$ are formal Laurent series

$$a_{-n} p^{-n} + a_{-n+1} p^{-n+1} + \cdots + a_0 + a_1 \cdot p + \cdots$$

We can write any elt. of $\mathbb{Q}_p$ as $p^{-n} \times$ an elt of $\mathbb{Z}_p$ for some n.

6.5.

Prop. We have an injection $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$. (Clear)

Def. Write $\mathbb{Z}_{(p)}$ for the localization of $\mathbb{Z}$ at the prime (p).

In other words fractions $\frac{a}{b}$ where $b \notin (p)$, i.e. $p \nmid b$.

Prop. We have an injection $\mathbb{Z}_{(p)} \hookrightarrow \mathbb{Z}_p$.

Proof. (Proof 1.) Given b, write $\frac{1}{b}$ as an elt. of $\mathbb{Z}_p$ as before.

Then, multiply by a. ($\mathbb{Z}_p$ is a ring)

(Proof 2.) Directly solve

$$\frac{a}{b} \equiv a_0 \pmod p$$

$$\frac{a}{b} \equiv a_0 + a_1 \cdot p \pmod{p^2}$$

$$\frac{a}{b} \equiv a_0 + a_1 \cdot p + a_2 \cdot p^2 \pmod{p^3}$$

etc.

The first one is possible because we can invert b.

For the second equation, know

$$a \equiv a_0 b + a_1 b p \pmod{p^2}$$

$$\underbrace{a - a_0 b}_{\text{divisible by } p} \equiv a_1 \cdot bp \pmod{p^2}$$

and we can divide by p, etc.

Ex. Write out a formal proof.

7.1.

Def. 1. A p-adic integer is a power series

$$a_0 + a_1 p + a_2 p^2 + \dots + a_n p^n + \dots$$

with each a_0 between 0 and $p-1$.

Prop. $\mathbb{Z}_p$ is a ring. (messy)

How we really think:

if α = above, $\alpha \equiv a_0 \pmod{p}$ really this is $\mathbb{Z}_p/(p)$

$\alpha \equiv a_0 + a_1 p \pmod{p^2}$

$\alpha \equiv a_0 + a_1 p + a_2 p^2 \pmod{p^2}$

and so α is determined by knowing what it is mod each p^k.

We have projections

$$\dots \longrightarrow \mathbb{Z}/p^4 \xrightarrow{\phi_3} \mathbb{Z}/p^3 \xrightarrow{\phi_2} \mathbb{Z}/p^2 \xrightarrow{\phi_1} \mathbb{Z}/p$$

and a p-adic number is smth that maps to all of them.

Def. $\mathbb{Z}_p := \varprojlim_n \mathbb{Z}/p^n$,

the inverse (projective) limit of $\mathbb{Z}/p^n$ w.r.t projection.

This means a p-adic integer is a sequence

$$\{b_1 \in \mathbb{Z}/p, b_2 \in \mathbb{Z}/p^2, b_3 \in \mathbb{Z}/p^3, \dots \}$$

such that $\phi_n(b_{n+1}) = b_n$ for all $n \geq 1$.

Notes. Each b_n determines b_k for $k < n$.

To make $\mathbb{Z}_p$ a ring, use the ring structure on the $\mathbb{Z}/p^i$.

1.2.

Prop. We have an injection $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$.

Proof. Given $a \in \mathbb{Z}$, take each b_k to be $a \pmod{p^k}$.

Note. If $a \geq 0$, for $p^k > a$ ~~there~~ we can represent a by ~~the same~~ $a \pmod{p^k}$ and $0 \leq a < p^k$.

So its power series representation writes it in base p.

If $a < 0$ this is not true.

Prop. We have an injection $\mathbb{Z}_{(p)} \hookrightarrow \mathbb{Z}_p$.

Proof. ETS $\frac{1}{a}$ maps into $\mathbb{Z}_p$ if $p \nmid a$.

If $p \nmid a$, then we can uniquely solve
$$a \cdot \bar{a}_1 \equiv 1 \pmod{p}$$
$$a \cdot \bar{a}_2 \equiv 1 \pmod{p^2}$$
$$a \cdot \bar{a}_3 \equiv 1 \pmod{p^3}$$
etc.

where each $\bar{a}_i \in \mathbb{Z}/p^i$.

Moreover, we have $\bar{a}_i \pmod{p^{i-1}} = \bar{a}_{i-1}$.
(by uniqueness)

So $\frac{1}{a}$ is the element $(\ldots, \bar{a}_3, \bar{a}_2, \bar{a}_1)$

and indeed $\underset{\overset{?}{=}(a,a,\ldots,a)}{a} \cdot (\ldots, \bar{a}_3, \bar{a}_2, \bar{a}_1) = (\ldots, 1, 1, 1)$
$= 1$.

Prop. $\mathbb{Z}_p \neq \mathbb{Z}_{(p)}$.

Proof 1. $\mathbb{Z}_p$ is uncountable (Cantor diagonalization)

Proof 2. Anything periodic is not in $\mathbb{Q}$ (prove)

Proof 3. (for $p = 2$ anyway)

If $\left(\frac{a}{p}\right) = 1$, show that $\sqrt{a} \in \mathbb{Z}_p$.
(Do by iteration.)

7.3. Proposition.

Let $F(x_1, \ldots, x_n)$ be a poly with integer coeffs.

Then, TFAE

1. $F(x_1, \cdots, x_n) \equiv 0 \mod p^v$ has a solution for all v.
2. $F(x_1, \ldots, x_n) = 0$ in $\mathbb{Z}_p$ has a solution.

Proof. (2) $\rightarrow$ (1) is a tautology.

Reduce everything (mod p^n). (i.e., take the map to $\mathbb{Z}/p^n$)

(1) $\rightarrow$ (2). Bogus proof.

Let $(x_1^{(1)}, \cdots, x_n^{(1)})$ be a solution mod p

$(x_1^{(2)}, \cdots, x_n^{(2)})$ mod p^2, etc.

and take $x_1 = (\cdots, x_1^{(3)}, x_1^{(2)}, x_1^{(1)})$ and so on.

Why is this bogus? [Explain.]

Correct proof: N, p. 105.

Another related definition.

$\mathbb{Z}_p$ is the ring together with maps $\mathbb{Z}_p \to \mathbb{Z}/p^n$ for each n, with the following "universal property":

Given ~~the maps~~ Y with maps from Y such that this commutes,

$$\begin{tikzcd}
\cdots \arrow[r] & \mathbb{Z}/p^4 \arrow[r, "\phi_3"] & \mathbb{Z}/p^3 \arrow[r, "\phi_2"] & \mathbb{Z}/p^2 \arrow[r, "\phi_1"] & \mathbb{Z}/p \\
& Y \arrow[u, "\psi_4"] \arrow[ur, "\psi_3"] \arrow[urr, "\psi_2"'] \arrow[urrr, "\psi_1"'] & & &
\end{tikzcd}$$

then there exists a ~~map~~ unique map $Y \longrightarrow \mathbb{Z}_p$ such that this commutes.

Proposition. $\mathbb{Z}_p$ exists.

Proof. Use the other definition.

7.4.

The p-adic absolute value.

We have an absolute value on $\mathbb{Q}$ induced by the map $\mathbb{Q} \hookrightarrow \mathbb{R}$.

We have another absolute value also.

For a given prime p, and $a \in \mathbb{Q}$, write $a = p^m \cdot \frac{b}{c}$ for some $m \in \mathbb{Z}$, b, c coprime to p.

Then the <u>p-adic valuation</u> of a, $v_p(a)$, is m.

Also write $v_p(0) = +\infty$.

<u>Lemma.</u>

(1) $v_p(a) = \infty \longleftrightarrow a = 0$.

(2) $v_p(a \cdot b) = v_p(a) + v_p(b)$.

(3) $v_p(a+b) \geq \min(v_p(a), v_p(b))$.

<u>Ex.</u> Write out a proof.

The <u>p-adic</u> <u>absolute</u> <u>value</u> $|a|_p$ is $|a|_p = p^{-v_p(a)}$.

Then:

(1) $|a|_p = 0 \longleftrightarrow a = 0$.

(2) $|a \cdot b|_p = |a|_p \cdot |b|_p$.

(3) $|a+b|_p \leq |a|_p + |b|_p$

in fact (3a) $|a+b|_p \leq \max(|a|_p, |b|_p)$.

(1), (2), (3) are the usual absolute value properties.

8.1.

[Recall: def. of p-adic valuation on $\mathbb{Q}$;

$v_p(a) = \infty \longleftrightarrow a = 0$

$v_p(a \cdot b) = v_p(a) + v_p(b)$

$v_p(a+b) \geq \min(v_p(a), v_p(b))$

$|a|_p = 0 \longleftrightarrow a = 0$

$|a \cdot b|_p = |a|_p \cdot |b|_p$

$|a+b|_p \leq |a|_p + |b|_p$

in fact,

$\leq \max(|a|_p, |b|_p)$.

(Do stuff on 8.2) (then come back)

Def. $\mathbb{Q}_p := \dfrac{\{\text{all Cauchy sequences}\}}{\{\text{Cauchy seq.} \to 0\}}$. (add elementwise)

Proposition.

(1) The absolute value $|\cdot|_p$ extends uniquely to $\mathbb{Q}_p$.

(2) $\mathbb{Q}_p$ is complete w.r.t. $|\cdot|_p$.

Proof. (1) Given $\alpha \in \mathbb{Q}_p$.

Then α is the limit of some Cauchy sequence $(x_1, x_2, x_3, \dots)$ in $\mathbb{Q}$ which does not converge to 0. (in $|\cdot|_p$).

This means, there exists $\varepsilon > 0$ such that the x_i do not all eventually satisfy $|x_i|_p < \varepsilon$.

For this ε, choose N s.t. $i, j > N \Rightarrow |x_i - x_j|_p < \varepsilon$.

Pick some $k > N$ s.t. $|x_k|_p \geq \varepsilon$.

Claim. If $i > N$ then $|x_i|_p = |x_k|_p$.

Proof. We have $|x_i|_p = |x_k + (x_i - x_k)|_p$

$\leq \max(|x_k|_p, |x_i - x_k|_p) = |x_k|_p$

and also $|x_k|_p = |x_i + (x_k - x_i)|_p$

$\leq \max(|x_i|_p, |x_k - x_i|_p)$ and soon get $|x_k|_p \leq |x_i|_p$.

(7.5) $\longrightarrow$ 8.2.

This allows us to talk about Cauchy sequences.

Recall. A Cauchy sequence w.r.t. $|\cdot|_p$ is a sequence $\{x_1, x_2, x_3, \dots\}$ in $\mathbb{Q}$ s.t. for any $\varepsilon > 0$, $\exists$ N s.t.

$$n, m \geq N \Longrightarrow |x_n - x_m|_p < \varepsilon.$$

The real numbers are the completion of $\mathbb{Q}$, we can define them as limits of Cauchy sequences.

In fact, $$\mathbb{R} := \frac{\{\text{all Cauchy sequences}\}}{\{\text{Cauchy seq. conv. to } 0\}}.$$

In p-adic land. Some Cauchy sequences:

$1, p, p^2, p^3, \dots \quad (\longrightarrow 0)$

$1, 1+p, 1+p+p^2, 1+p+p^2+p^3 \quad (\longrightarrow 1+p+p^2+\dots)$

$a_0, a_0 + a_1 p, a_0 + a_1 p + a_2 p^2, \dots \quad$ (for any a_0, a_1, a_2)

(back to 8.1)

See where this is going?

This gives us $\mathbb{Q}_p$.

Then $\mathbb{Z}_p \overset{\text{(expand)}}{:=} \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$.

(the valuation ring)

So we define $|x|_p = |x_i|_p$ for each $i > N$.

Ex. Check that the p-adic absolute value properties ~~agree~~ hold for $\mathbb{Q}_p$, and this absolute value agrees w.r.t. $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$. (diagonal emb.)

Why is $\mathbb{Q}_p$ complete?

Sketch of proof.

Given a Cauchy sequence

$$(x_1, x_2, x_3, \cdots) \quad \text{in } \mathbb{Q}_p,$$

choose a sequence

$$(y_1, y_2, y_3, \cdots) \quad \text{in } \mathbb{Q}$$

where $|x_i - y_i|_p \le p^{-i}$.

(Can do because $\mathbb{Q}_p$ is p-adic limits in $\mathbb{Q}$)

Also a Cauchy sequence.

Then, writing $y = \lim_{i\to\infty} y_i$, check that also $y = \lim_{i\to\infty} x_i$.

Def. Write $\mathbb{Z}_p := \{ x \in \mathbb{Q}_p : |x|_p \le 1 \}$.

(This is the same as the previous $\mathbb{Z}_p$, as we will prove.)

Prop. $\mathbb{Q}_p$ is a field and $\mathbb{Z}_p$ is a ring.

Proof. $\mathbb{Q}_p$ a field is mildly annoying.

Add and multiply and divide Cauchy sequences elementwise.

(Note: If $(x_1, x_2, x_3, \dots) \not\to 0$, maybe some x_i are zero but eventually they're not. So cut off the beginning.)

Check that this preserves Cauchy sequences.

$\mathbb{Z}_p$ a ring? This is easy: $|x+y|_p \le \max(|x|_p, |y|_p)$.

Exercise. $\mathbb{Z}_p$ is the closure of $\mathbb{Z}$ in $\mathbb{Q}_p$.

§.4.

Prop. 1. The units $\mathbb{Z}_p^\times$ are $\{x \in \mathbb{Z}_p : |x|_p = 1\}$.

2. The maximal ideal is $\{x \in \mathbb{Z}_p : |x|_p < 1\}$

and this is (p).

3. The ideals of $\mathbb{Z}_p$ are (0) and (p^n) for $n \geq 1$.

4. $\mathbb{Z}_p/(p^n) \xrightarrow{\sim} \mathbb{Z}/(p^n)$.

Proof. (1) Given $x \in \mathbb{Z}_p$. Then $\exists\, y \in \mathbb{Q}_p$ s.t. $x \cdot y = 1$.

Then $|x|_p \leq 1$.

$$|x|_p \cdot |y|_p = |1|_p = 1.$$

So $|y|_p \leq 1 \longleftrightarrow |x|_p = 1$.

(2) Clear that this is an ideal and that it's maximal.

Must have $|x|_p \leq \frac{1}{p}$ and so $x = p \cdot (\text{sth in } \mathbb{Z}_p)$.

(3) Given an ideal $\underline{a}$, let $x \in \underline{a}$ of smallest possible valuation v.

$$\text{Then } x \cdot \mathbb{Z}_p = p^v \cdot \underbrace{\left(\frac{x}{p^v}\right)}_{\text{a unit}} \mathbb{Z}_p$$

and so $(p^v) \subseteq \underline{a}$.

Conversely $\underline{a} \subseteq (p^v)$ by hypothesis.

(4) Consider $\mathbb{Z} \longrightarrow \mathbb{Z}_p / p^n \mathbb{Z}_p$.

Has kernel $p^n \mathbb{Z}$,

and is surjective because given $x \in \mathbb{Z}_p$,

can write $x = x_1 + x_2$

x_1: an integer; x_2: in $p^n\mathbb{Z}_p$ (has abs. value $\leq p^{-n}$.)

8.9.) **Prop.**

We have an isomorphism

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

(completion construction) (inverse limit construction)

Moreover: Give "completion" $\mathbb{Z}_p$ the metric topology.
"inverse limit" $\mathbb{Z}_p$ the inverse limit topology:

Basis generated by:

~~tac~~ $\mathbb{Z}/p^4 \xrightarrow{\phi_3} \mathbb{Z}/p^3 \xrightarrow{\phi_2} \mathbb{Z}/p^2 \xrightarrow{\phi_1} \mathbb{Z}/p$

Regard p-adics as sets ~~all elts~~ $(\dots, x_4, x_3, x_2, x_1)$

For any n and any x_n,
$\{$all p-adics with x_n in slot $n\}$
is an open set,
and these generate the topology.

Then this map is also a homomorphism.

Proof. We have $\mathbb{Z}_p/(p^n) \cong \mathbb{Z}/(p^n)$,
so the map is determined by mapping $x \in \mathbb{Z}_p$ to
$(\dots, x \bmod p^3, x \bmod p^2, x \bmod p)$.

Preserves ring structure on each $\mathbb{Z}/p^n$, hence on their inverse limit.

(Also: A sequence as at right is Cauchy.)

Topology. A basis is $\{x \in \mathbb{Z}_p : |x - x_0| < \varepsilon\}$.
WLOG can take $\{x \in \mathbb{Z}_p : |x - x_0| \leq p^{-n}\}$ for all $n \geq 0$

$= \{x_0 + p^n \mathbb{Z}_p : x_0 \in \mathbb{Z}_p\}$.

Precisely what we have on the right.

9.2. Some cool facts.

Prop. (the product formula) If $0 \neq a \in \mathbb{Q}$, then

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

Proof. Write $a = \pm \prod_{p \neq \infty} p^{v_p}$.

Then $|a|_p = p^{-v_p}$ and $|a|_\infty = \pm a$.

$$\text{So} \prod_{p \leq \infty} |a|_p = \prod_{p < \infty} |a|_p \cdot |a|_\infty$$

$$= \prod_p p^{-v_p} \cdot |a| = \frac{|a|}{|a|} = 1 .$$

Prop. $\mathbb{Z}_p$ is compact.

Can define a Haar measure: $\mu(\mathbb{Z}_p) = 1$,

$\mu(p\mathbb{Z}_p) = \frac{1}{p}$ by additive invariance.

Indeed, can extend this measure to $\mathbb{Q}_p$.

$\mu(\frac{1}{p}\mathbb{Q}_p) = p$, etc.

Can do analysis over $\mathbb{Q}_p$ (Tate's thesis)

Solving equations

Example. Show $x^2 + 5y^2 = 2$ has no solutions in $\mathbb{Q}_5$.

(and, thus, no solutions in $\mathbb{Q}$)

Proof. Let $a = v_p(x)$ and $b = v_p(y)$.

Then, $v_p(x^2) = 2a$

$v_p(5y^2) = 2b + 1$.

Recall $v_p(u+v) \geq \min(v_p(u), v_p(v))$

with equality when these are different.

9.3. Proof? Write $u+v = p^c r + p^d s$ with $r, s \in \mathbb{Z}_p^\times$ and WLOG $c < d$.

$$= p^c(r + p^{d-c}s).$$

Then $r + p^{d-c}s$ is also in $\mathbb{Z}_p^\times$ and not in $p\mathbb{Z}_p$.

So: $v_p(x^2 + 5y^2) = \min(2a, 2b+1) = 0$

and so $a = 0$ and $b \geq 0$.

So if $x^2 + 5y^2 = 2$ in $\mathbb{Q}_5$, then in fact,

$x^2 + 5y^2 = 2$ in $\mathbb{Z}_5$ (and, moreover, $5 \nmid x$.)

Recall $\mathbb{Z}_5 / 5\mathbb{Z}_5 \cong \mathbb{Z}/5$.

Reduce mod 5!

$x^2 \equiv 2 \pmod 5$. (nope.)

The Hasse-Minkowski theorem.

A quadratic form has solutions in $\mathbb{Q}$

$\longleftrightarrow$ it does in all $\mathbb{Q}_p$.

Solving equations

Ex. Solve $x^2 \equiv 2$ in $\mathbb{Z}_7$.

Can we do it?

Write $x = (\cdots, x_3, x_2, x_1)$ as an inverse limit.

Then $x_1 = 3$ or 4. Say 3.

$x_2 = 7a_2 + 3$.

$$(7a_2 + 3)^2 = 2 \quad (\text{in } \mathbb{Z}/49)$$
$$14a_2 + 9 = 2$$
$$14a_2 = -7$$
$$2a_2 = -1$$
$$a_2 = \bar{2} \cdot -1 = -4 = 3.$$

Exists and uniquely det.

(9.4.) = 10.1.

Suppose we have found $x_n \in \mathbb{Z}/7^n$.

Write $x_{n+1} = 7^n \cdot a_{n+1} + \underbrace{a_n}$.

Here we pick a lift to $\mathbb{Z}$. choice doesn't matter, except a_{n+1} depends on it.

Solve $(7^n \cdot a_{n+1} + a_n)^2 = 2$ in $\mathbb{Z}/7^{n+1}$

$$\underbrace{7^{2n} \cdot a_{n+1}^2}_{0.} + 7^n \cdot 2a_{n+1} + a_n^2 = 2$$

$$7^n \cdot 2a_{n+1} = \underbrace{2 - a_n^2}$$

This is $\equiv 0 \pmod{7^n}$.

$$2a_{n+1} = \frac{2 - a_n^2}{7^n}$$

$$a_{n+1} = \bar{2} \cdot \frac{2 - a_n^2}{7^n}.$$

This keeps working iteratively, so $\sqrt{2} \in \mathbb{Z}_7$.

Theorem. Let $n \in \mathbb{Z}$, coprime to p. Then, for $p > 2$,

$$\sqrt{n} \in \mathbb{Z}_p \longleftrightarrow \left(\frac{n}{p}\right) = 1.$$

(Note: If n is not coprime to p, only take square roots if div. by square factors.) $\sqrt{p} \notin \mathbb{Z}_p$.

10.

Theorem. (Hensel's Lemma)

Given a polynomial $f(x)$ in $\mathbb{Z}[x]$ (or $\mathbb{Z}_p[x]$), not all coeffs divisible by p.

Suppose $f(x) \equiv \bar{g}(x)\bar{h}(x) \mod p$, where $\bar{g}, \bar{h}$ coprime.

Then, there is a factorization

$$f(x) = g(x)\,h(x)$$

reducing to above mod p.

(9.5) The cool special case of Hensel's lemma.
$=10.2.$

Suppose $f(x) \in \mathbb{Z}[x]$ has a root α mod p.
Suppose also $f'(\alpha)$ is not zero.
Then $f(x)=0$ has a solution β in $\mathbb{Z}_p$ s.t.
$\beta \pmod p = \alpha$.

Why is this a special case?

all in $\mathbb{Z}/p$. [Write $f(x) = (x-\alpha)g(x)$.
If also $x-\alpha \mid g(x)$ then $f'(\alpha)=0$ in $\mathbb{Z}/p$.

Proof. Lift from $\mathbb{Z}/p$ to $\mathbb{Z}/p^2$ to $\mathbb{Z}/p^3$, etc.
Let $f(x) = \sum_i a_i x^i$.
Suppose $f(b) = \sum a_i b^i = 0$ in $\mathbb{Z}/p^n$. (Lift b arbitrarily to $\mathbb{Z}/p^{n+1}$)
Look for a solution $b + cp^n$ in $\mathbb{Z}/p^{n+1}$.

Try to solve:
$$\sum_{i=0}^{k} a_i (b+cp^n)^i = 0 \text{ in } \mathbb{Z}/p^{n+1}$$
$$\sum a_i b^i + p^n\left[a_1 \cdot c + 2a_2 \cdot b \cdot c + 3a_3 b^2 \cdot c + \cdots + (k) a_k b^{k-1} \cdot c\right]$$
$$= 0 \text{ in } \mathbb{Z}/p^{n+1}$$

$$\underbrace{\sum a_i b^i}_{\text{know this is divisible by } p^n} + p^n \cdot c\left[a_1 + 2a_2 b + 3a_3 b^2 + \cdots + k a_k b^{k-1}\right] = 0$$

So if $a_1 + 2a_2 b + \cdots + k a_k b^{k-1} = f'(b) \neq 0$ in $\mathbb{Z}/p^{n+1}$,
then can solve for c, and moreover
$$cp^n = -\frac{f(b)}{f'(b)}.$$
So replace b with $b + cp^n = b - \dfrac{f(b)}{f'(b)}$.

(Jump around and act really excited)

Can make this more like Newton's lemma.

Suppose $\alpha_1 \in \mathbb{Z}_p$ s.t. $|f(\alpha_1)|_p \le \frac{1}{p}$.

Then, replacing α_1 with $\alpha_2 := \alpha_1 - \frac{f(\alpha_1)}{f'(\alpha_1)}$

we get $|f(\alpha_2)|_p \le \frac{1}{p^2}$.

Iterating, $|f(\alpha_n)|_p \le \frac{1}{p^n}$.

(Ex. The convergence is in fact faster. Prove this.)

Let $\alpha = \lim_{n\to\infty} \alpha_n$. (which exists!)

Then $f(\alpha) = \lim_{n\to\infty} f(\alpha_n) = 0$.

<u>General form</u>: Not as pretty, so omitted.

Applications.

<u>Ex</u>. A number $x \in \mathbb{Q}$ is a square iff it is a square in $\mathbb{Q}_p$ for every p.

<u>Proof</u>. Don't go back to first principles!

$\longrightarrow$ is obvious.

But, in fact, $x = \pm \prod_{p<\infty} p^{v_p(x)}$.

So, a square if and only if all the v_p's are even.

Proving nonexistence of rational solutions.

(1) $X^2 + Y^2 + Z^2 = 0$

(2) $3X^2 + 2Y^2 - Z^2 = 0$.

(3) $X^2 - 3Y^2 = 0$.

<u>Claim</u>. None of them have nontrivial solutions.

10.4.

(1) Look over $\mathbb{R}$. (done)

(2) Look over $\mathbb{Q}_3$ (equivalently, $\mathbb{Z}_3$)

WLOG, not all ~~coprime~~ divisible by 3.

Mod 3: $2Y^2 - Z^2 \equiv 0 \pmod 3$.

So $Y \equiv Z \equiv 0 \bmod 3$.

This means $X \equiv 0 \bmod 3$ also.

(because $v_3(2Y^2 - Z^2) \geq 2$

so $v_3(3X^2) \geq 2$.

Contradiction. (Fermat's descent)

(3a). Look over $\mathbb{Q}_3$ again. (This is familiar)

(3b). No solutions in $\mathbb{Q}_7$.

If there is a solution in $\mathbb{Z}_7^\times$,

get $\{1, 2, \text{or } 4\} - \{3, 6, \text{or } 5\}$. Doesn't work!

Can get a 0 in one slot but not both.

A subtler example.

$$(x^2 - 2)(x^2 - 17)(x^2 - 34) = 0$$

has a root in $\mathbb{Q}_p$ for all $p \leq \infty$, but not in $\mathbb{Q}$.

Exercise. Prove it.

Here's the interesting part. Let $p \neq 2, 17, \infty$.

Then $\left(\frac{2}{p}\right) = 1 \longleftrightarrow x^2 - 2$ has a root in $\mathbb{Q}_p$

$\left(\frac{17}{p}\right) = 1 \longleftrightarrow x^2 - 17$ "

$\left(\frac{34}{p}\right) = 1 \longleftrightarrow x^2 - 34$.

10.5. A still harder example.

Show $X^4 - 17 = 2Y^2$ has solutions in all $\mathbb{Q}_p$ not in $\mathbb{Q}$.

(An elliptic curve. Ш is nontrivial.)

This idea does have one triumph though.

Theorem. (Hasse-Minkowski)

Let $F(x_1, \cdots, x_n) \in \mathbb{Q}[x_1, \cdots, x_n]$ be a quadratic form. (homo poly of deg 2)

Then $F(x_1, \cdots, x_n) = 0$ has nontrivial solutions in $\mathbb{Q}$ $\longleftrightarrow$ it has nontrivial solutions in every $\mathbb{Q}_p$.

11.1. Applications of p-adic numbers.

Theorem. (Hasse - Minkowski)

Let $F(x_1, \dots, x_n) \in \mathbb{Q}[x_1, \dots, x_n]$ be a quadratic form.

Then $F(x_1, \dots, x_n) = 0$ has solutions in $\mathbb{Q}$

$\longleftrightarrow$ it does in $\mathbb{Q}_p$ for all $p \le \infty$

Note. Write V for the equ $F(x_1, \dots x_n) = 0$
(an algebraic variety)

Can say $V(\mathbb{Q}) = \phi \longleftrightarrow \prod_{p \le \infty} V(\mathbb{Q}_p) = \phi$

$\longleftrightarrow \prod_{p \le \infty} V(\mathbb{A}_{\mathbb{Q}}) = \phi$. adeles.

Won't prove all of it. (See Serre, Course on Arith.)

n=1. $F(x) = ax^2 = 0$. Nope, no nontrivial solutions.
~~WLOG, solve $x^2 = 0$~~

n=2. $F(x) = ax_1^2 + bx_2^2 = 0$.

Note. If $F(x) = ax_1^2 + cx_1x_2 + bx_2^2$,
$F(x) = a(x_1 + \frac{c}{2a}x_2)^2 + (b - \frac{c^2}{4a^2})x$
so equivalent.

WLOG, $F(x) = x_1^2 + bx_2^2 = 0$.
and, indeed, $b < 0$ if we want to solve over $\mathbb{R}$.

So write $x_1^2 - bx_2^2 = 0$ which says b is a square.

If we write $b = \prod_p p^{v_p(b)}$,

b is a square in $\mathbb{Q} \longleftrightarrow v_p(b)$ is even for all p $(p \ne \infty)$

$\updownarrow$

$b \in \mathbb{Q}_p^2$ for all p.

$n = 3$.

By linear algebra, can diagonalize:

$$f = x_1^2 - a x_2^2 - b x_3^2. \quad \text{(no assumption on sign of } a, b.)$$

Proposition. ~~Let $k = \mathbb{R}$ or $\mathbb{Q}_p$.~~ in $\mathbb{Q}_p$

The equation is solvable nontrivially in $\mathbb{Q}_p$ iff a is the norm of an element of ~~k~~ $\mathbb{Q}_p(\sqrt{b})$.

Also. Same is true if $\mathbb{Q}_p$ is replaced by $\mathbb{Q}$.

Proof. (Serre, p. 19 — "Hilbert symbol")

Case 1. If $b = c^2$ in $\mathbb{Q}_p$ then $\mathbb{Q}_p(\sqrt{b}) = \mathbb{Q}_p$, so "$a$ is a norm" just says $a \in \mathbb{Q}_p$, which is automatically true.

And, indeed, $c^2 - a \cdot 0^2 - b \cdot 1^2 = 0$.

Case 2. $b \neq c^2$ in $\mathbb{Q}_p$, and $\mathbb{Q}_p(\sqrt{b})$ is a quadratic ext.

Can write every $\xi \in \mathbb{Q}_p(\sqrt{b})$ as $z + \sqrt{b}\, y$ $\quad (y, z \in \mathbb{Q}_p)$

$$N(\xi) = z^2 - b y^2.$$

So, if a is a norm, $a = z^2 - by^2$, and

$$z^2 - a \cdot 1^2 - b \cdot y^2 = 0.$$

Conversely, if $z^2 - ax^2 - by^2 = 0$, have $x \neq 0$ (because b not a square)

and $a = N\left(\frac{z}{x} + \sqrt{b}\,\frac{y}{x}\right)$.

Note. This was a digression but illustrates, norms from extensions are important.

11.3.

Have $f = x_1^2 - ax_2^2 - bx_3^2$. WLOG, a, b squarefree, integers!
Also WLOG, $|a| \le |b|$.

Induct on $m := |a| + |b|$.

$m = 0, 1, 2$. Finite computation (skipped).

Assume $m > 2$.

Write $b = \pm p_1 \cdots p_k$; let p be one of the p_i.

Claim. a is a square mod p (if the eqn is solvable).

Note. Implies a is a square mod $b = \prod p_i$. (CRT)

Proof of claim. If $a \equiv 0 \bmod p$ obvious.

Otherwise, $0 = z^2 - ax^2 - by^2$ for some x, y, z primitive (coprime)

$$z^2 - ax^2 \equiv 0 \pmod p.$$

Now $x \not\equiv 0 \bmod p$.

(Because, if $p \mid x$, then $p \mid z$ also, and $p \mid y$, so solution not prim.)

So $x \not\equiv 0$, so a is a square mod p.

Therefore: There exist integers t, b' with

$$t^2 = a + bb'$$

satisfying $|t| \le \frac{|b|}{2}$.

(Restriction on t? Any t in a fixed residue class mod b works, take the smallest.)

$$bb' = t^2 - a = (t - \sqrt{a})(t + \sqrt{a})$$

and so bb' is a norm of $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$ or $\mathbb{Q}_p(\sqrt{a})/\mathbb{Q}_p$.

11.4.

Now, since bb' is a norm,

b is a norm $\longleftrightarrow$ b' is a norm.

(Norms are multiplicative)

So, $x_1^2 - ax_2^2 - bx_3^2$ represents 0

$\updownarrow$

$x_1^2 - ax_2^2 - b'x_3^2$ represents 0.

(This is true in $\mathbb{Q}$ or in $\mathbb{Q}_p$.)

But $|b'| = \left|\frac{t^2-a}{b}\right| \le \left|\frac{t^2}{b}\right| + \left|\frac{a}{b}\right|$

$\le \frac{|b|}{4} + 1 < |b|$.

Now write $b' = b''u^2$ where u is an integer (perhaps $u=1$)

and so on. result follows by induction.

$n=4$. Use some results. Break up into sum of two forms

$n=5$. Induction. (Uses some more serious theory.)

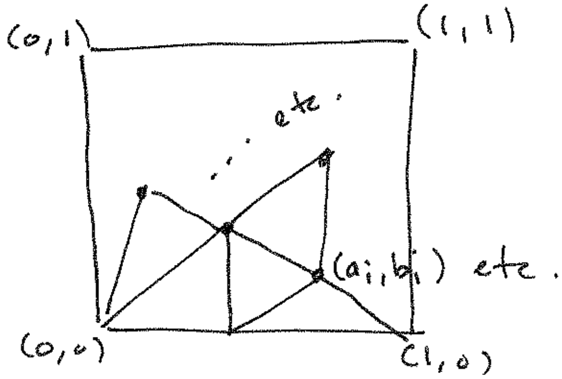
Another cool result. (Monsky, On dividing a square into triangles)

Theorem. Given a square, it cannot be divided into an odd number of nonoverlapping triangles, all of the same area.

11.5.

Sketch of proof.

Suppose first coordinates are rational.



Call a vertex (x,y) Type A : $|x|_2 < 1$, $|y|_2 < 1$

Type B : $|x|_2 \geq 1$, $|x|_2 \geq |y|_2$

Type C : $|y|_2 \geq 1$, $|y|_2 < |x|_2$.

Lemmas.

(1) No line, or triangle of area $\frac{1}{m}$ (m odd) can contain vertices of all three types.

(2-adic computations; area)

(2) Some triangle must contain vertices of all three types.

(Count the number of A-B edges in the square; then do some elementary combinatorics.)

If coordinates are not rational.

Extend $|\cdot|_2$ to $\mathbb{R}$.

This is really weird. Use Zorn's Lemma.

Or extend it to the extension gen. by the coordinates.