Abstract. These are the rough ongoing lecture notes for the course 18.782 (Introduction to Arithmetic Geometry) taught at MIT in Fall 2019. The notes will be updated each weekend, following the lectures during the week. Be sure to clear your cache before reloading in order to get the most current version of the notes. If you find any typos/mistakes in the notes, please let me know!

1. Lecture 1

Note: This lecture is intended to be informal and motivational. It discusses several outside concepts (such as Riemann surfaces) which are not strictly needed in the remainder of the course. The lecture also briskly introduces several algebro-geometric concepts in an informal manner, to give intuition; all of these will be reintroduced more slowly and rigorously later in the semester.

1.1. Historical context. A Diophantine equation is a polynomial equation with integral (or rational) coefficients:

\[ f(x_1, \ldots, x_n) = 0, \quad f \in \mathbb{Z}[x_1, \ldots, x_n]. \]

Diophantus of Alexandria (c. 200-300 AD) wrote a series of texts called *Arithmetica* examining the problem of solving such equations in the integers or the rationals. Given \( f \) as above and a commutative ring \( R \), let us denote

\[ V_f(R) = \{ P \in R^n : f(P) = 0 \}. \]

Diophantine analysis is the study of the relationship between Diophantine equations \( f = 0 \) and the sets \( V_f(\mathbb{Z}) \) or \( V_f(\mathbb{Q}) \). Below are some examples of Diophantine equations, which were mentioned by Fermat in his 1650 letter to Carcavi summarizing Fermat’s earlier works:

- For \( p \) odd prime, \( x^2 + y^2 = p \) is solvable in integers \( (x, y) \in \mathbb{Z}^2 \) if and only if \( p \equiv 1 \mod 4 \) (Fermat’s two-square theorem, proved by Euler around 1750).
- For every \( k \in \mathbb{Z}_{\geq 1} \), the equation \( x^2 + y^2 + z^2 + w^2 = k \) is solvable in integers (Lagrange’s four-square theorem, proved by Lagrange in 1770).
- For every positive nonsquare integer \( N \), the equation \( x^2 - Ny^2 = 1 \) is solvable in integers (Pell’s equation; its solvability goes back to work of Brahmagupta c. 600-700 AD).
- \( x^3 + y^3 = z^3 \) has no solution in positive integers (the \( n = 3 \) case of the so-called Fermat’s Last Theorem; this case was proved by Euler in 1770).
- The only integral solutions of \( y^2 = x^3 - 2 \) are \( (x, y) = (\pm 3, 5) \).

(Fermat rarely gave proofs of his claims, and sometimes made incorrect ones.) The study of these and other Diophantine equations (especially involving binary quadratic forms) drove much of the research in number theory in the period following Fermat, and in particular formed the foundations for the development of algebraic number theory.

On the other hand, given an equation \( f = 0 \) as above, we can view the aggregate of its complex solutions \( V_f(\mathbb{C}) \) as a geometric object, namely a (complex) algebraic variety. *Algebraic geometry* is the field devoted to studying the geometric properties of algebraic varieties as well as their interactions with algebraic properties of the defining equations.

*Date: September 16, 2019.*
Arithmetic geometry is a relatively modern field of mathematics one of whose aims is to build a bridge between the geometric objects $V_f(\mathbb{C})$ and the arithmetic objects $V_f(\mathbb{Z})$ (or $V_f(\mathbb{Q})$). The fact that there should be a connection between the two aspects of the equation $f = 0$ is surprising and adds to the allure of the subject.

Below, we will briefly discuss some of the achievements in the twentieth century, to illustrate the role of geometry in the study of Diophantine equations. Suppose we are given a nonconstant polynomial $f = f(x,y) \in \mathbb{Q}[x,y]$. Since the set $V_f(\mathbb{R})$ of real points on the real affine plane $\mathbb{A}^2(\mathbb{R}) = \mathbb{R}^2$ typically, forms a one-dimensional object, we refer to $V_f$ as an affine plane curve defined over $\mathbb{Q}$. Let us make the two assumptions about $f$:

- $V_f$ is geometrically irreducible, i.e. $f$ is irreducible as a polynomial in $\mathbb{C}[x,y]$, and
- $V_f$ is nonsingular, i.e. $\nabla f(P) = (\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P)) \neq 0$ for every $P \in V_f(\mathbb{C})$.

Under these hypotheses, the set of complex points $V_f(\mathbb{C})$ admits the structure of a connected Riemann surface (i.e. complex manifold of dimension 1). In the informal discussion that follows, it will be useful for us to consider the “projective curve” $\overline{V}_f$ obtained by “compactifying” $V_f$ by adding a finite number of “points at infinity” (we will also assume nonsingularity at these points). Then $\overline{V}_f(\mathbb{C})$ is a closed Riemann surface, which is topologically characterized by its genus $g$ or number of “doughnut holes” on the surface. We have the following basic trichotomy, in differential geometric terms:

- ($g = 0$). $\overline{V}_f(\mathbb{C})$ is topologically a sphere. It can be given a complete Riemannian metric of constant positive curvature, so as to be “positively curved.” Its Euler characteristic is positive: $\chi > 0$.
- ($g = 1$). $\overline{V}_f(\mathbb{C})$ is topologically a torus. It can be given a complete Riemannian metric of constant zero curvature, so as to be “flat” (like the world as imagined by Pacman.) Its Euler characteristic is zero: $\chi = 0$.
- ($g \geq 2$). $\overline{V}_f(\mathbb{C})$ can be given a complete Riemannian metric of constant negative curvature, so as to be “negatively curved” (like on the surface of a saddle.) Its Euler characteristic is negative: $\chi < 0$.

Suppose now that $\overline{V}_f(\mathbb{Q})$ is nonempty. (This is a highly nontrivial assumption!) We then have the following trichotomy in the behavior of $\overline{V}_f(\mathbb{Q})$.

- ($g = 0$). $\overline{V}_f(\mathbb{Q})$ is infinite.
- ($g = 1$). $\overline{V}_f(\mathbb{Q})$ has the structure of an abelian group; and this group is in fact finitely generated. This latter statement was conjectured by Poincaré in 1901; it was proved by Mordell in 1921, with generalization by Weil in 1928.
- ($g \geq 2$). $\overline{V}_f(\mathbb{Q})$ is finite. This was conjectured by Mordell in 1923, and proved by Faltings in 1983, which led to his 1986 Fields medal.

Thus, the trichotomy of curvature in geometry reverberates in arithmetic!

1.2. Rational points on conics. Let us consider the problem of finding rational solutions to Diophantine equations of degree 2 in two variables (i.e. equations of conics). Our analysis will serve to illustrate the utility of geometric intuition in solving Diophantine problems.

Example 1. Let us determine $V_f(\mathbb{Q})$ where

\[ f(x,y) = x^2 + y^2 - 1. \]

Note that the set $V_f(\mathbb{R})$ of real solutions to equation (1) forms a unit circle in the real affine plane $\mathbb{A}^2(\mathbb{R}) = \mathbb{R}^2$. The rational solutions correspond to the points on the unit circle with rational $x$- and $y$-coordinates.
To determine $V_f(\mathbb{Q})$, first note that $(-1,0)$ lies in $V_f(\mathbb{Q})$. If $(x,y)$ is any other rational point in $V_f(\mathbb{Q})$, then the line joining $(-1,0)$ to $(x,y)$ has rational slope. Conversely, a line of rational slope $t \in \mathbb{Q}$ through $(-1,0)$ intersects $V_f$ at exactly one other point $(x_t, y_t)$, and this point is rational. Indeed, note that $(x_t, y_t)$ solves simultaneously the equations

$$x^2 + y^2 = 1 \quad \text{and} \quad y = t(x + 1).$$

Substitution gives us

$$x^2 + t^2(x + 1)^2 = 1 \implies (x + 1)((1 + t^2)x - (1 - t^2)) = 0.$$

If $x = -1$ then $y = 0$, which is excluded. If $x \neq 0$, we see that

$$(x_t, y_t) = \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right).$$

Therefore, we have

$$V_f(\mathbb{Q}) = \left\{\left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right) : t \in \mathbb{Q}\right\} \cup \{(-1,0)\}.$$

Note that we may informally view $(-1,0)$ as the point obtained by letting the parameter $t$ “tend to infinity;” indeed, note that

$$\lim_{|t| \to \infty} \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right) = (-1,0).$$

To give a cleaner presentation of $V_f(\mathbb{Q})$, it will be useful to work with projective curves, which are introduced below.

Fix a base field $k$ (say $\mathbb{Q}$). The projective $n$-space $\mathbb{P}^n$ over $k$ is defined by setting, for each field extension $L/k$,

$$\mathbb{P}^n(L) = \frac{L^{n+1} \setminus \{(0, \cdots, 0)\}}{\sim}$$

where the equivalence relation $\sim$ on $L^{n+1} \setminus \{(0, \cdots, 0)\}$ is given by

$$(a_0, \cdots, a_n) \sim (b_1, \cdots, b_n)$$

if and only if $(a_0, \cdots, a_n) = (\lambda \cdot b_1, \cdots, \lambda \cdot b_n)$ for some $\lambda \in L^\times$. Note that $\mathbb{P}^n(L)$ may be viewed as the space of lines through the origin (more precisely, one-dimensional vector subspaces) in the vector space $L^{n+1}$ over $L$. Given $a_0, \cdots, a_n \in L$ not all zero, we shall denote the class of $(a_0, \cdots, a_n)$ in $\mathbb{P}^n(L)$ by $[a_0 : \cdots : a_n]$.

**Example 2.** As a set,

$$\mathbb{P}^1(L) = \{[1 : a] : a \in L\} \cup \{[0 : 1]\} = L \sqcup \{\infty\}.$$

For example, $\mathbb{P}^1(\mathbb{C})$ is the Riemann sphere giving a one-point compactification of the complex plane $\mathbb{C}$. In general, we have

$$\mathbb{P}^n(L) = \{[1 : a_1 : \cdots : a_n] : a_i \in L\} \sqcup \{[0 : a_1 : \cdots : a_n] : a_i \in L\} = \mathbb{A}^n(L) \sqcup \mathbb{P}^{n-1}(L).$$

Thus, $\mathbb{P}^n$ may be viewed as a “compactification” of the affine space $\mathbb{A}^n$ obtained by adding $\mathbb{P}^{n-1}$ “at infinity.”

For a homogeneous polynomial $F(X_0, X_1, X_2) \in \mathbb{Q}[X_0, X_1, X_2]$ of degree $d \geq 1$ and field extension $L/\mathbb{Q}$, the zero set

$$V_F(L) = \{(a_0 : a_1 : a_2) \in \mathbb{P}^2(L) : F(a_0, a_1, a_2) = 0\}$$

is well-defined, since $F(\lambda X_0, \lambda X_1, \lambda X_2) = \lambda^d F(X_0, X_1, X_2)$ for every $\lambda \in L^\times$. We refer to $V_F$ as a projective curve defined over $\mathbb{Q}$. 

3
Example 3. Let \( f(x, y) = x^2 + y^2 - 1 \) as in Example 1. The zero set \( V_f(\mathbb{C}) \) in \( \mathbb{P}^2(\mathbb{C}) \) of the homogenization
\[
F(X_0, X_1, X_2) = X_0^2 f \left( \frac{X_1}{X_0}, \frac{X_2}{X_0} \right) = X_1^2 + X_2^2 - X_0^2
\]
is given by the union of two sets
\[
\{ [1 : a_1 : a_2] \in \mathbb{P}^2(\mathbb{C}) : F(1, a_1, a_2) = f(a_1, a_2) = 0 \} = V_f(\mathbb{C})
\]
and
\[
\{ [0 : a_1 : a_2] \in \mathbb{P}^2(\mathbb{C}) : F(0, a_1, a_2) = a_1^2 + a_2^2 = 0 \} = \{ (0 : 1 : i), (0 : 1 : -i) \}.
\]
Thus, we have
\[
V_F(\mathbb{C}) = V_f(\mathbb{C}) \cup \{ (0 : 1 : i), (0 : 1 : -i) \}
\]
and we may view \((0 : 1 : i)\) and \((0 : 1 : -i)\) as points “at infinity” of \( V_f \) in \( \mathbb{P}^2 \). Note that we have a well-defined map
\[
\mathbb{P}^1(\mathbb{C}) \to V_F(\mathbb{C}) \subseteq \mathbb{P}^2(\mathbb{C})
\]
given by
\[
(t_0 : t_1) \mapsto \left( t_0^2 + t_1^2 : t_0^2 - t_1^2 : 2t_0 t_1 \right),
\]
which in fact establishes a bijection between (the complex points and) rational points of \( \mathbb{P}^1 \) and \( V_F \). Note that the restriction of the map above to the affine line \( \mathbb{A}^1 = \{ [1 : t] \} \subseteq \mathbb{P}^1 \) can be written
\[
t = (1 : t) \mapsto (1 + t^2 : 1 - t^2 : 2t) = \left( 1 : \frac{1 - t^2}{1 + t^2} : \frac{2t}{1 + t^2} \right) = \left( \frac{1 - t^2}{1 + t^2} : \frac{2t}{1 + t^2} \right)
\]
which agrees with the rational parametrization given in Example 1. We will later revisit this example and show that the map given above is an isomorphism of algebraic curves over \( \mathbb{Q} \), so we may write
\[
\mathbb{P}^1 \simeq V_F.
\]

It is easy to see that, although our discussion was limited to a particular conic section \( x^2 + y^2 = 1 \), the same argument can be used a to give a rational parametrization of rational points for an arbitrary nondegenerate conic section, provided that it has at least one rational point to begin with. This leads to the following result:

**Theorem 4.** Let \( C \) be a geometrically irreducible (smooth) projective curve of degree 2 in \( \mathbb{P}^2 \) defined over \( \mathbb{Q} \). Then the following are equivalent:

1. \( C(\mathbb{Q}) \) is nonempty.
2. \( C \simeq \mathbb{P}^1 \) over \( \mathbb{Q} \).

This naturally leads us to the problem of finding necessary and sufficient conditions for a curve \( C \) as above to have a rational point. This will be solved by the Hasse-Minkowski theorem, which will be covered in later lectures.

2. Lecture 2

2.1. Absolute values.

**Definition 5.** An absolute value on a field \( K \) is a function
\[
| \cdot | : K \to \mathbb{R}_{\geq 0}
\]
such that, for all \( x, y \in K \),
- \(|x| = 0 \iff x = 0 \)
- \(|xy| = |x| \cdot |y| \)
- \(|x + y| \leq |x| + |y| \) (triangle inequality)
If $| \cdot |$ satisfies the strong triangle inequality
\[ |x + y| \leq \max\{|x|, |y|\} \]
for all $x, y \in K$, then $| \cdot |$ is nonarchimedean; otherwise, it is archimedean.

**Example 6.** We have the following.

1. The usual absolute value on $\mathbb{R}$ or $\mathbb{C}$, and its restriction to subfields.
   We shall denote by $| \cdot |_\infty$ the restriction of this to $\mathbb{Q}$.
2. The trivial absolute value on any field $K$ is defined by
   \[ |x| = \begin{cases} 1 & x \neq 0, \\ 0 & x = 0. \end{cases} \]

We will construct new absolute values $| \cdot |_p$ on $\mathbb{Q}$ for each prime number $p$. By the Fundamental Theorem of Arithmetic, for each $n \in \mathbb{Q}^\times$ there exist unique $u \in \{\pm 1\}$ and $n_2, n_3, n_4, \ldots \in \mathbb{Z}$ (indexed by primes, with all but finitely many $n_p$ zero) such that
\[ n = u \prod_{p \text{ prime}} p^{n_p}. \]

**Definition 7.** For each prime $p$, the $p$-adic valuation on $\mathbb{Q}$ is the function
\[ v_p : \mathbb{Q}^\times \to \mathbb{Z} \]
given by $v_p(n) = n_p$. We extend $v_p$ to a function $v_P : \mathbb{Q} \to \mathbb{Z} \cup \{+\infty\}$ by setting $v_p(0) = +\infty$.

**Lemma 8.** For any prime $p$ and $x, y \in \mathbb{Q}$, we have
\[ v_p(xy) = v_p(x) + v_p(y) \]
\[ v_p(x + y) \geq \min\{v_p(x), v_p(y)\} \]

Proof. (1) and (2) are clear. To prove (3), we may assume $x \neq 0$ and $y \neq 0$ since otherwise the claim is clear (note that $+\infty \geq n$ for any $n \in \mathbb{Z}$) by convention. Let us write $x = p^u \frac{z}{s}$ and $y = p^v \frac{u}{r}$ with $u, v, r, s \in \mathbb{Z}$ not divisible by $p$. WLOG, $v_p(x) = n \leq m = v_p(y)$. Then
\[ x + y = p^n \left( \frac{r}{s} + p^{m-n} \frac{u}{v} \right) = \frac{p^n rv + p^{m-n} us}{sv}. \]
Since $p \mid sv$, it follows that $v_p(x + y) \geq v_p(x) = \min\{v_p(x), v_p(y)\}$ as desired. \qed

**Corollary-Definition 9.** The function $| \cdot |_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ given by $|x|_p = p^{-v_p(x)}$ is a nonarchimedean absolute value, called the $p$-adic absolute value on $\mathbb{Q}$.

**Remark.** Note the product formula: for every $x \in \mathbb{Q}^\times$, we have $\prod_{p\in\mathbb{P}} |x|_p = 1$.

2.2. **Completions.** Let $K$ be a field with absolute value $| \cdot |$.

**Definition 10.** A sequence $(a_i)$ in $K$
\[ (a) \text{ converges to } \ell \in k \text{ if for all } \epsilon > 0 \text{ there exists } N \geq 0 \text{ such that } |a_i - \ell| < \epsilon \text{ for all } i \geq N. \]
\[ (b) \text{ is Cauchy if } \forall \epsilon > 0 \text{ there exists } N \text{ such that } |a_i - a_j| < \epsilon \text{ for all } i, j \geq N. \]

Note that every convergent sequence is Cauchy. We say that $K$ is complete with respect to $| \cdot |$ if every Cauchy sequence converges in $K$.

**Example 11.** $\mathbb{Q}$ is not complete with respect to the usual absolute value $| \cdot |_{\infty}$, but $\mathbb{R}$ is.

**Definition 12.** Two sequences $(a_i)$ and $(b_i)$ in $K$ are equivalent if $\lim_{i \to \infty} |a_i - b_i| = 0$.

**Definition 13.** The completion $\hat{K}$ of $K$ with respect to $| \cdot |$ is the set of equivalence classes of Cauchy sequences in $K$. 

5
Note that $\hat{K}$ forms a field with respect to termwise addition and multiplication:

\[
[(a_i)] + [(b_i)] = [(a_i + b_i)],
\]

\[
[(a_i)] \cdot [(b_i)] = [(a_i \cdot b_i)].
\]

The additive identity in $\hat{K}$ is the class $0 = [(0,0,0,\ldots)]$ and the multiplicative identity is the class $1 = [(1,1,1,\ldots)]$. If $(a_i)$ is a Cauchy sequence in $K$ and $(a_i) \sim 0$, then there exists $N \geq 0$ such that $a_i \neq 0$ for all $i \geq N$. So defining

\[
b_i = \begin{cases} 0 & i \leq 0, \\ a_i^{-1} & i \geq N \end{cases}
\]

we see that $[(a_i)] \cdot [(b_i)] = [(0,\ldots,0,1,1,\ldots)] = 1$ so $[(a_i)]$ is invertible.

Let $\| \cdot \| : \hat{K} \to \mathbb{R}_{\geq 0}$ be the function given by $\|(a_i)\| = \lim_{i \to \infty} |a_i|$. Then $\| \cdot \|$ is an absolute value on $\hat{K}$, and $\hat{K}$ is complete with respect to $\| \cdot \|$. The restriction of $\| \cdot \|$ to $K$ under the embedding $K \hookrightarrow \hat{K}$ given by $a \mapsto [(a,a,\ldots)]$ recovers the original absolute value $|\cdot|$ on $K$. In the absence of confusion, we will use the same notation for the absolute value on $\hat{K}$ and the absolute value on $K$. Finally, note that if $(a_i)$ is a Cauchy sequence in $K$ and $a = [(a_i)]$ denotes its class in $\hat{K}$, then

\[
\lim_{i \to \infty} a_i = a \text{ in } \hat{K}.
\]

**Proposition 14.** Let $L$ be a field complete with respect to an absolute value $|\cdot|$, and let $K \subset L$ be an arbitrary subfield (so that $K$ inherits an absolute value from $L$).

1. The inclusion $K \subset L$ extends uniquely to a field embedding $\hat{K} \hookrightarrow L$.

2. If every element of $L$ is a limit of a sequence in $K$, then $\hat{K} \simeq L$.

**Proof.** The embedding $\hat{K} \to L$ is given by $[(a_i)] \mapsto \lim_{i \to \infty} a_i$. \(\square\)

**Definition 15.** For each prime $p$, the field $\mathbb{Q}_p$ of $p$-adic numbers is the completion of $\mathbb{Q}$ with respect to the $p$-adic absolute value $|\cdot|_p$.

2.3. Ostrowski’s theorem.

**Definition 16.** Two absolute values $|\cdot|, |\cdot|'$ on a field $K$ are **equivalent** if there is a real number $\alpha > 0$ such that

\[
|x|' = |x|^\alpha
\]

for every $x \in K$.

**Remark.** If two absolute values $|\cdot|$ and $|\cdot|'$ on $K$ are equivalent, then they have the same completions $(\hat{K},|\cdot|) \simeq (\hat{K},|\cdot|')$.

**Theorem 17** (Ostrowski). Up to equivalence, the nontrivial absolute values on $\mathbb{Q}$ are precisely the $p$-adic absolute values $|\cdot|_p$ for $p$ prime and $|\cdot|_\infty$.

**Proof.** Let $\| \cdot \|$ be an absolute value on $\mathbb{Q}$. By multiplicativity of $\| \cdot \|$, it suffices that $\| \cdot \|$ agrees on $\mathbb{Z}_{\geq 1}$ with the trivial absolute value or $|\cdot|_p^\alpha$ for some $\alpha > 0$ and $p \leq \infty$. We have three cases:

**Case 1.** Suppose there exists $b \in \mathbb{Z}_{\geq 1}$ with $\|b\| > 1$.

Let $b$ be the smallest such. Note that $b \geq 2$ since $|1| = 1$. Let $\alpha > 0$ be a real number such that $|b| = b^\alpha = |b|_\infty^\alpha$. For any $n \in \mathbb{Z}_{\geq 1}$, let us write

\[
n = a_0 + a_1 b + \cdots + a_s b^s, \quad 0 \leq a_i < b, \quad b^s \leq n < b^{s+1}.
\]
Then we have

\[ \|n\| \leq \|a_0\| + \|a_1\|\|b\| + \cdots + \|a_s\|\|b\|^s \]

\[ \leq 1 + b^\alpha + \cdots + b^{\alpha s} \quad \text{(since } \|a_i\| \leq 1 \text{ by minimality of } b) \]

\[ = (1 + b^{-\alpha} + \cdots + b^{-\alpha s})b^{\alpha s} \]

\[ \leq cn^\alpha \]

for some constant \( c > 0 \) independent of \( n \). We have here used the observation that \( 1 + b^{-\alpha} + \cdots + b^{-\alpha s} \) is a partial sum of the geometric series \( \sum_{i=0}^{s} b^{-\alpha i} \) which is (absolutely) convergent whence bounded, since \( 0 < b^{-\alpha} < 1 \). Thus, for each integer \( N \geq 1 \), if we apply the above argument to \( n^N \) we obtain

\[ \|n^N\| \leq c(n^N)^\alpha \iff \|n\| \leq c^{1/N}n^{\alpha}. \]

Letting \( N \to \infty \), we thus deduce \( \|n\| \leq n^{\alpha} \) for every \( n \in \mathbb{Z}_{\geq 1} \). Next, noting that

\[ \|b^{s+1}\| \leq \|b^{s+1} - n\| + \|n\| \]

we have

\[ \|n\| \geq \|b^{s+1}\| - \|b^{s+1} - n\| \]

\[ \geq b^{(s+1)\alpha} - (b^{s+1} - n)^\alpha \quad \text{(by what we proved earlier)} \]

\[ \geq b^{(2s+1)\alpha} - b^{(s+1)\alpha} = b^{(s+1)\alpha}\left(1 - \left(1 - \frac{1}{b}\right)^\alpha\right) \]

\[ \geq cn^\alpha \]

for some constant \( c > 0 \) independent of \( n \). Applying the same argument as above, we find that \( \|n\| \geq n^{\alpha} \) for every \( n \in \mathbb{Z}_{\geq 1} \). Thus \( \|n\| = n^{\alpha} \) for every \( n \in \mathbb{Z}_{\geq 1} \).

**Case II.** Suppose \( \|n\| = 1 \) for every \( n \in \mathbb{Z}_{\geq 1} \). Then \( \| \cdot \| \) is the trivial absolute value.

**Case III.** Suppose \( \|n\| \leq 1 \) for every \( n \in \mathbb{Z}_{\geq 1} \), and \( \|b\| < 1 \) for some \( b \in \mathbb{Z}_{\geq 1} \).

Let \( b \) be the smallest such. Then \( b \) must be a prime number (say \( p \)), since if \( b = rs \) with \( r, s \in \mathbb{Z}_{\geq 1} \) then \( 1 > \|b\| = \|r\|\|s\| \) which implies \( \|r\| < 1 \) or \( \|s\| < 1 \), implying \( b = r \) or \( b = s \) by minimality of \( b \). We now claim that \( \|q\| = 1 \) for every prime \( q \neq p \). Indeed, if \( \|q\| < 1 \) then, for every \( N \geq 1 \), by coprimality of \( p^N \) and \( q^N \) there exist \( u, v \in \mathbb{Z} \) such that

\[ 1 = up^N + vq^N \]

which implies

\[ 1 \leq \|u\|\|p\|^N + \|v\|\|q\|^N \leq \|p\|^N + \|q\|^N. \]

Taking \( N \) to be sufficiently large, we obtain a contradiction; hence, \( \|q\| = 1 \) for any prime \( q \neq p \).

Now, let \( \alpha > 0 \) be a real number such that \( \|p\| = p^{-\alpha} = |p|^{\alpha} \). Then for any \( n \in \mathbb{Z}_{\geq 1} \) we have

\[ \|n\| = \prod_{q} q^{v_q(n)} \|p\|^{v_p(n)} = p^{-\alpha v_p(n)} = |n|^{\alpha}. \]

\[ \square \]

3. Lecture 3

**Definition 18.** A discrete valuation on a field \( K \) is a function

\[ v : K \to \mathbb{Z} \cup \{+\infty\} \]

such that, for all \( x, y \in K \),

- \( v(x) = +\infty \iff x = 0 \)
- \( v(xy) = v(x) + v(y) \)
- \( v(x + y) \geq \min\{v(x), v(y)\} \)
Example 19. We have the following examples.

- The $p$-adic valuation $v_p$ on $\mathbb{Q}$ extends to a discrete valuation on $\mathbb{Q}_p$ by $v_p(x) = -\log_p |x|_p$.
- Let $C(t)$ be the field of rational functions in one variable $t$ over $C$. For every $a \in C$, the function
  
  $v_a(f) = \text{order of vanishing of } f \text{ at } a \quad f \in C(t)^*$

  is a discrete valuation on $C(t)$.

- The trivial valuation on $K$ is given by $v(x) = 0$ for any $x \in K^*$.

Definition-Lemma 20. Let $v : K \to \mathbb{Z}$ be a nontrivial discrete valuation.

(a) The valuation ring of $v$ is $O_v = \{x \in K : v(x) \geq 0\}$.
(b) $O_v$ has a unique maximal ideal $m_v = \{x \in K : v(x) > 0\}$ and $O_v^\times = O_v \setminus m_v$.
(c) $m_v$ is principal. Any $\pi \in m_v$ such that $m_v = \pi O_v$ is called a uniformizer of $O_v$. Every nonzero ideal of $O_v$ is of the form $\pi^k O_v$ for some $k \geq 0$.
(d) We have Frac $O_v = K$, and in fact $O_v[\frac{1}{\pi}] = K$. The field $k_v = O_v/m_v$ is called the residue field of the valuation.

Proof. (a) Since $v(0) = +\infty$ and $v(1) = 0$, we have $0, 1 \in O_v$. If $x, y \in O_v$ so $v(x), v(y) \geq 0$, then $v(xy) = v(x) + v(y) \geq 0$ and $v(x + y) \geq \min\{v(x), v(y)\} \geq 0$ so $xy \in O_v$ and $x + y \in O_v$. This shows that $O_v$ is a subring of $K$.

(b) Arguing as in (a), we see that $m_v$ is an ideal of $O_v$. If $x \in O_v \setminus m_v$, then $v(x) = 0$ which implies that

$$v\left(\frac{1}{x}\right) = v\left(\frac{1}{x}\right) + v(x) = v(1) = 0$$

so that $1/x \in O_v$ and $x \in O_v^\times$. It follows that $O_v^\times = O_v \setminus m_v$, the inclusion $O_v^\times \subseteq O_v \setminus m_v$ being obvious. This shows that $m_v$ is the unique maximal ideal of $O_v$, as desired. (Recall that $R^\times = R \setminus \bigcup_{m \in R} \text{maximal ideal } m$ for any commutative ring $R$.)

(c) Let $\pi \in m_v$ be any element such that $v(\pi) = \min\{v(x) : x \in m_v\}$. Then for any $x \in m_v$,

$$v\left(\frac{x}{\pi}\right) = v(x) - v(\pi) \geq 0 \implies x/\pi \in O_v \implies x \in \pi O_v.$$

This shows that $m_v = \pi O_v$. In fact, for any $x \in m_v$ we have $v(x/\pi) = 0$ or $x/\pi \in m$ (and in particular $v(x/\pi) \geq v(\pi)$ by minimality of $v(\pi)$). By an inductive argument, we conclude that $v(\pi) | v(x)$ for every $x \in m_v$. So if $I \subseteq O_v$ is any nonzero ideal, then $\min\{v(x) : x \in I\} = k \cdot v(\pi)$ for some $k \in \mathbb{Z}_{>0}$, and $I = \pi^k O_v$ by arguing as above.

We remark that, by the argument above, each nonzero $x \in O_v$ can be written in the form $\pi^k u$ where $k = v(x)/v(\pi) \in \mathbb{Z}_{>0}$ and $u \in O_v^\times$.

(d) Let $\pi \in O_v$ be a uniformizer. For any $x \in K$, we have $v(\pi^N x) = N v(\pi) + v(x) \geq 0$ for $N \gg 0$ and hence $\pi^N x \in O_v$ and $x \in O_v[1/\pi]$.

3.2. $p$-adic integers.

Definition 21. The ring $\mathbb{Z}_p$ of $p$-adic integers is the valuation ring of $\mathbb{Q}_p$ with respect to $v_p$:

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : v_p(x) \geq 0\} = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$ 

Proposition 22. The following is immediate from the previous subsection.

(1) The unique maximal ideal of $\mathbb{Z}_p$ is $p\mathbb{Z}_p$.
(2) The group of $p$-adic units of $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus p\mathbb{Z}_p$.
(3) Every $x \in \mathbb{Z}_p$ is of the form $p^n u$ with $n = v_p(x) \in \mathbb{Z}_{\geq 0}$ and $u \in \mathbb{Z}_p^\times$.

Proposition 23. The ring $\mathbb{Z}_p$ is the $p$-adic closure of $\mathbb{Z}$ in $\mathbb{Q}_p$. In other words:

(1) If $a = \lim_{i \to -\infty} a_i$ in $\mathbb{Q}_p$ with $a_i \in \mathbb{Z}$, then $a \in \mathbb{Z}_p$. 

(2) For every $a \in \mathbb{Z}_p$, there is a sequence $(a_i)$ with $a_i \in \mathbb{Z}$ such that $a = \lim_{i \to \infty} a_i$ in $\mathbb{Q}_p$.

Proof. (1) If $\lim_{i \to \infty} a_i = a$ with $a_i \in \mathbb{Z}$, then $|a_i|_p = \lim_{i \to \infty} |a_i|_p \leq 1$.

(2) Let $a \in \mathbb{Z}_p$ be given, and write $a = \lim_{i \to \infty} a_i$ with $a_i \in \mathbb{Q}$. Since $\lim_{i \to \infty} |a_i| = |a|_p \leq 1$ and $| \cdot |_p$ takes values in $p^\mathbb{Z}$, we see that $a = 0$ or $|a|_p$ must be eventually constant with $|a|_p \leq 1$ for $i \gg 0$. Thus, we may assume without loss of generality that $|a|_p \leq 1$ for all $i$. Let us write

$$a_i = \frac{b_i}{c_i} \quad \text{with } b_i, c_i \in \mathbb{Z} \text{ such that } \gcd(b_i, c_i) = 1 \text{ and } p \nmid c_i.$$

For each $i \geq 1$, by coprimality of $p^i$ and $c_i$ there exist $u_i, v_i \in \mathbb{Z}$ such that $b_i = u_i p^i + v_i c_i$. Then

$$a_i = \frac{u_i p^i + v_i c_i}{c_i} = v_i + p^i \frac{u_i}{c_i} \implies |a_i - v_i|_p = \left| p^i \frac{u_i}{c_i} \right|_p \leq p^{-i}.$$

This shows that $(v_i) \sim (a_i)$ and $\lim_{i \to \infty} v_i = \lim_{i \to \infty} a_i = a$. \hfill \Box

Proposition 24 (p-adic expansion). We have the following.

(a) Every $a \in \mathbb{Z}_p$ can be written uniquely in the form

$$a = b_0 + b_1 p + b_2 p^2 + \ldots, \quad b_i \in \{0, \ldots, p - 1\}.$$

Conversely, any series of the form $\sum_{i=0}^{\infty} b_i p^i$ with $b_i \in \{0, \ldots, p - 1\}$ converges in $\mathbb{Z}_p$.

(b) Each $a \in \mathbb{Q}_p$ can be written in the form

$$a = \sum_{i=k}^{\infty} b_i p^i, \quad b_i \in \{0, \ldots, p - 1\}$$

for some $k \in \mathbb{Z}$ such that $v_p(a) = \min\{i : b_i \neq 0\}$.

Proof. (a) Let $a \in \mathbb{Z}_p$ be given. By Proposition 23, there exists $b'_0 \in \mathbb{Z}$ such that $|a - b'_0|_p < 1$. Then $a = b'_0 + p a'_1$ for some $a'_1 \in \mathbb{Z}_p$. Moreover, writing $b'_0 = pq + b_0$ with $q \in \mathbb{Z}$, $b_0 \in \{0, \ldots, p - 1\}$ and $a_1 = a'_1 + q$, we thus can write

$$a = b_0 + pa_1, \quad b_0 \in \{0, \ldots, p - 1\}, a_1 \in \mathbb{Z}_p.$$

Moreover, $b_0$ and $a_1$ are uniquely determined by $a$. Indeed, if we have $b_0 + pa_1 = p' a''_1 + a''_1$ with $b'_0 \in \{0, \ldots, p - 1\}$ and $a''_1 \in \mathbb{Z}_p$, then $b_0 - b'_0 = p(a''_1 - a_1)$ showing that $b_0 - b'_0$ is an integer with $|b_0 - b'_0|_p < p$ satisfying $v_p(b_0 - b'_0) > 0$, and therefore $b_0 = b'_0$ and $a_1 = a''_1$. Similarly, we can write $a_1$ uniquely as

$$a_1 = b_1 + pa_2, \quad b_1 \in \{0, \ldots, p - 1\}, a_2 \in \mathbb{Z}_p.$$

Note then that $a = b_0 + b_1 p + p^2 a_2$ with $a_2 \in \mathbb{Z}_p$. By recursion we obtain a sequence $\{b_0, b_1, b_2, \ldots\}$ of elements in $\{0, \ldots, p - 1\}$ such that the sequence of partial sums $\{b_0, b_0 + b_1 p, b_0 + b_1 p + b_2 p^2, \ldots\}$ is Cauchy and converges to $a$.

(b) This follows from the fact that $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$. \hfill \Box

Lemma 25. For each $n \geq 1$, the inclusion $\mathbb{Z} \to \mathbb{Z}_p$ induces a natural isomorphism

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

compatible with the projections

$$\begin{array}{ccc}
\mathbb{Z}/p^{n+1} \mathbb{Z} & \cong & \mathbb{Z}/p^n \mathbb{Z} \\
\downarrow & & \downarrow \\
\mathbb{Z}_p/p^{n+1} \mathbb{Z}_p & \cong & \mathbb{Z}_p/p^n \mathbb{Z}_p
\end{array}$$

Proof. The class of $a = \sum_{i=0}^{\infty} b_i p^i \in \mathbb{Z}_p$ in $\mathbb{Z}_p/p^n \mathbb{Z}_p$ is the same as the class of $a' = \sum_{i=0}^{n} b_i p^i \in \mathbb{Z}$, so the homomorphism $\mathbb{Z} \to \mathbb{Z}_p/p^n \mathbb{Z}_p$ is surjective. The kernel of this surjection is $\mathbb{Z} \cap p^n \mathbb{Z}_p = p^n \mathbb{Z}$. \hfill \Box
3.3. \( \mathbb{Z}_p \) as an inverse limit.

**Definition 26.** An *inverse system* of sets is a sequence \((A_n)\) of sets and maps \((f_n)\) of the form

\[
\cdots \to A_{n+1} \xrightarrow{f_n} A_n \to \cdots \to A_2 \xrightarrow{f_1} A_1 \xrightarrow{f_0} A_0.
\]

The *inverse limit* \( A = \varprojlim A_n \) of such an inverse system is given by

\[
A = \left\{ (a_n) \in \prod_{n=0}^{\infty} A_n : f_n(a_{n+1}) = a_n \text{ for all } n \geq 0 \right\}
\]
equipped with projections \( \epsilon_n : A \to A_n \) such that \( \epsilon_n = f_n \circ \epsilon_{n+1} \) for all \( n \geq 0 \).

**Remark.** If \( \{(A_n), (f_n)\} \) is an inverse system of groups (resp. rings) with group homomorphisms (resp. ring homomorphisms), then \( \varprojlim A_n \) naturally has the structure of a group (resp. ring).

**Example 27.** The sequence of projections \( \cdots \to \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z} \to \cdots \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \) forms an inverse system of rings.

**Proposition 28.** The projections \( \mathbb{Z}_p \to \mathbb{Z}_p/p^n\mathbb{Z}_p \) induce an isomorphism

\[
\mathbb{Z}_p \simeq \varprojlim \mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \varprojlim \mathbb{Z}/p^n\mathbb{Z}.
\]

**Proof.** Under the natural map \( \mathbb{Z}_p \to \varprojlim \mathbb{Z}_p/p^n\mathbb{Z}_p \), each element \( ([b_0], [b_0+b_1p], [b_0+b_1p+b_2p^2], \ldots) \in \varprojlim \mathbb{Z}_p/p^n\mathbb{Z}_p \) is in the image of \( \sum_{i=0}^{\infty} b_ip^i \in \mathbb{Z}_p \). The kernel of this map is \( \bigcap_n p^n\mathbb{Z}_p = \{0\} \). \( \square \)

**Remark.** An alternative but equivalent way to build up the \( p \)-adic numbers \( \mathbb{Q}_p \) is to first define \( \mathbb{Z}_p \) as the inverse limit \( \varprojlim \mathbb{Z}/p^n\mathbb{Z} \) and define \( \text{Frac}(\mathbb{Z}_p) = \mathbb{Q}_p \). This is the approach taken e.g. in the notes of Poonen in the 2009 version of this course.