p-adic Groups

Yuval Gat
(+972) 58-5896580*

HUJI 2022/23, Winter Semester

Abstract

Advanced course in p-adic groups, taught by prof. Ori Parzanchevski. The course should be accessible even to mature third-year B.Sc. students; some Galois theory may be required, but not much more. Exercises will be given every three to four weeks, with a large assignment at the end.

Contents

[*] Feel free to message me regarding any mistake you may find.

0 Introduction

We start with some motivating questions. Consider the equation $x^3 + y^3 = z^3$, and we're looking for solutions in $\mathbb{Q}$ or $\mathbb{Z}$, and not in $\mathbb{R}$. This is an example of a *diophantine equation.* Another relevant question, proposed by Fermat, asks when a prime p is a sum of two squares. The solution is that p is a sum of two squares if and only if $p = 2$ or $p \equiv 1 \pmod 4$. The easy direction can be proved as follows. If $p \equiv 3 \pmod 4$ and $p = a^2 + b^2$ for $a, b \in \mathbb{Z}$, then $a^2 + b^2 \equiv 3 \pmod 4$; this is impossible, since the square of every integer is either 0 or $1 \pmod 4$.

If a diophantine equation has a solution in $\mathbb{Z}$, it has a solution in $\mathbb{F}_p$ for any prime p, and also in $\mathbb{Z}/m\mathbb{Z}$ for any $m \in \mathbb{N}$. Is the converse true?

Question: If a diophantine equation has a solution in $\mathbb{Z}/m\mathbb{Z}$ for any $m \in \mathbb{N}$ and in $\mathbb{R}$, does it have a solution in $\mathbb{Z}$?

Answer: It depends. Examples will be given later.

Theorem (Chinese Remainder Theorem)**.** *There exists a solution in $\mathbb{Z}/m\mathbb{Z}$ for all m if there exists a solution in $\mathbb{Z}/p^k\mathbb{Z}$ for any prime p and natural k. The following isomorphism of rings holds:*

$$m = \prod p_i^{k_i} \implies \mathbb{Z}/m\mathbb{Z} \cong \prod \left(\mathbb{Z}/p_i^{k_i}\mathbb{Z}\right)$$

Goal: Study polynomial equations in $\mathbb{Z}/p^k\mathbb{Z}$. Consider, for example, $x^2 \equiv -1 \pmod 2$; there exists a solution, $x = 1$. There is no solution for $x^2 \equiv -1 \pmod 4$.

Lemma 1 (Hensel's Lemma)**.** *Let $f(x) \in \mathbb{Z}[x]$, and p be any prime. If there exists $a_0 \in \mathbb{F}_p$ with $f(a_0) \equiv 0 \pmod p$, and $f'(a_0) \not\equiv 0 \pmod p$, then f is solvable in $\mathbb{Z}/p^k\mathbb{Z}$ for any k. Moreover, there exist $a_k \in \mathbb{Z}/p^{k+1}\mathbb{Z}$ such that $f(a_k) \equiv 0 \pmod{p^{k+1}}$ and $a_k \equiv a_{k-1} \pmod{p^k}$.*

Example 1. Consider $f(x) = x^2 + 1, p = 2$. Then $f(1) = 0$ but $f'(1) = 0$ so we cannot apply the lemma. Consider $p = 5, a_0 = 2$. Then $f(a_0) = 2^2 + 1 \equiv 0 \pmod 5$, but $f'(a_0) = 2 \cdot 2 = 4 \not\equiv 0 \pmod 5$. Thus $x^2 \equiv -1 \pmod{5^k}$ is always solvable: $a_0 = 2, a_1 = 7, a_2 = 57$ etc. In base 5:

$$[a_0]_5 = 2, [a_1]_5 = 12, [a_2]_5 = 212, [a_3]_5 = 1212, [a_4] = 31212, ...$$

Indeed, the lemma tells us that in base p, digits are added on the left for the next a_k.

Proof of Hensel's Lemma. By induction, assume the claim for $k - 1$, i.e. that $a_{k-1} \in \mathbb{Z}/p^k\mathbb{Z}$ and $f(a_{k-1}) \equiv 0 \pmod{p^k}$. We are looking for a_k such that $f(a_k) \equiv 0 \pmod{p^{k+1}}$, and $a_k \equiv a_{k-1} \pmod{p^k}$, that is, $a_k = x \cdot p^k + a_{k-1}$ and $x \in \{0, 1, \ldots, p-1\}$. We solve for x.

Recall Taylor's theorem: for $f \in \mathbb{R}[x]$, $f(a + x) = f(a) + f'(a)x + \frac{1}{2}f''(a)x^2 + \cdots$. This is a finite sum, because f is a polynomial. If we replace $\mathbb{R}$ by $\mathbb{Z}$, it can be observed that $\frac{f^{(n)}(a)}{n!} \in \mathbb{Z}$. Also notice $n! \mid \frac{(n+k)!}{k!}$.

The following expansion thus has integral coefficients:

$$0 \overset{p^{k+1}}{\equiv} f(a_k) = f(a_{k-1} + xp^k) =$$
$$f(a_{k-1}) + f'(a_{k-1})xp^k + \frac{1}{2}f''(a_{k-1})x^2p^{2k} + \cdots + \frac{f^{(\deg f)}(a_{k-1})}{\deg f!}x^{\deg f}p^{k \deg f}$$

All terms after p^{2k} vanish because we work modulo p^{k+1}. We thus need to solve:

$$p^k f'(a_{k-1})x \equiv -f(a_{k-1}) \pmod{p^{k+1}}$$

Notice both sides are divisible by p^k, so $f'(a_{k-1})x \equiv -\frac{f(a_{k-1})}{p^k} \pmod p$. By our assumption, we can divide, $x \equiv -\frac{f(a_{k-1})/p^k}{f'(a_{k-1})} \pmod p$. The division in the numerator is done in $\mathbb{Z}$. We can also write $f'(a_0)$ in the denominator by the compatibility of the solutions, and 'division' by it means finding an inverse in $\mathbb{Z}/p\mathbb{Z}$. □

Consequences: After choosing a_0, the sequence of solutions is unique. Furthermore, we found an algorithm to construct these:

$$a_k = a_{k-1} - f(a_{k-1}) \cdot f'(a_0)^{-1}$$

where the inverse is taken in $\mathbb{Z}/p\mathbb{Z}$. Also note this inverse is computed once. This is Newton's approximation method! The $\mathbb{Z}/p^k\mathbb{Z}$ can be thought of as 'better and better' approximations of $\mathbb{Z}$.

Say $f \in \mathbb{Z}[x]$ and there exists $a_0 \in \{0, \ldots, 9\}$ with $f(a_0) \equiv 0 \pmod{10}$ and $f'(a_0) \not\equiv 0 \pmod{10}$. Does Hensel's Lemma work? We want $(a_k)_{k=0}^{\infty}$ with $f(a_k) \equiv 0 \pmod{10^{k+1}}$ and $a_k \equiv a_{k-1} \pmod{10^k}$. This fails at the last step of the proof: we can't divide by the derivative. This works, however, if we require $f'(a_0) \in (\mathbb{Z}/10\mathbb{Z})^{\times}$; this is the general form of Hensel's Lemma - we required the derivative be invertible in the ring, i.e. coprime to the p in question (10 in our example).

Example 2. Consider $x^2 + 31 \equiv 0 \pmod{10^k}$. It has solutions for all k, and they are compatible: $a_k \equiv a_{k-1} \pmod{10^k}$. To show this we need a slightly stronger version of Hensel's Lemma. In any case, the solutions are $3, 03, 603, 4603, 74603, \ldots$. We want to say this sequence 'converges' in some useful sense. For this, we need a new metric, under which the sequence converges to an element of the ring we will study - the 10-adic integers.

1 The p-adic Numbers

Definition 1 (The n-adic Integers)**.** Define $\mathbb{Z}_n = \{\sum_{k=0}^{\infty} d_k \cdot n^k : 0 \le d_k \le n-1\}$. This is a ring, with the usual addition and multiplication (with carrying etc.)

Note $\mathbb{N}$ is embedded in $\mathbb{Z}_n$ as $\{\sum_{k=0}^{N} d_k n^k : N \in \mathbb{N}\}$ (infinitely many zeros to the left). Actually, $\mathbb{Z}$ is embedded in $\mathbb{Z}_n$; for example, the additive inverse of 3657 is $\cdots 99996343$. The negatives are thus embedded as the numbers with infinitely many 9's to the left.

In our earlier example, we had the 10-adic number $\cdots 74603$. Squaring this, we should get -31, or $\cdots 999969$.

Lemma 2 (Hensel's Lemma for the n-adic Integers)**.** *If $f \in \mathbb{Z}[x]$, $f(a_0) \equiv 0 \pmod{n}$, $f'(a_0) \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ then $f(x) = 0$ is solvable in $\mathbb{Z}_n$.*

Observe there's a ring homomorphism $\mathbb{Z}_n \to \mathbb{Z}/n^k\mathbb{Z}$ for any k:

$$\sum_{i=0}^{\infty} d_i n^i \overset{\mu_k}{\mapsto} \sum_{i=0}^{k-1} d_i n^i$$

This is a homomorphism due to the way we defined addition and multiplication in $\mathbb{Z}_n$. We denote the image of $\alpha \in \mathbb{Z}_n$ under μ_k by $\alpha \pmod{n^k}$. These maps are compatible in the sense that the following diagram commutes[1] for $\ell < k$:

$$\begin{tikzcd}
 & \mathbb{Z}/n^k\mathbb{Z} \\
\mathbb{Z}_n \arrow[ur, "\mu_k"] \arrow[dr, "\mu_\ell"'] & \\
 & \mathbb{Z}/n^\ell\mathbb{Z} \arrow[uu]
\end{tikzcd}$$

Let $f \in \mathbb{Z}[x]$ and a_k such that $f(a_k) \equiv 0 \pmod{10^{k+1}}$, $a_k \equiv a_{k-1} \pmod{10^k}$. Define $\alpha = \sum_{k=0}^{\infty} \lfloor \frac{a_k}{10^k} \rfloor 10^k \in \mathbb{Z}_{10}$. Observe $\alpha \equiv a_k \pmod{10^{k+1}}$. Since μ_k are homomorphisms, $f(\alpha) \equiv f(a_k) \equiv 0 \pmod{10^{k+1}}$, and this is true for every k. Thus $f(\alpha) = 0$. We thus found a root for f. In fact, the converse also holds: f has a root in $\mathbb{Z}_n$ if and only if there exists a_k such that $f(a_k) \equiv 0 \pmod{10^{k+1}}$ and $a_k \equiv a_{k-1} \pmod{10^k}$. It is in fact true that the last assumption about the compatibility can be dropped.

Question: What elements of $\mathbb{Z}_n$ have inverses?

[1] In fact, this establishes $\mathbb{Z}_n$ as the inverse limit of $\mathbb{Z}/n^k\mathbb{Z}$ together with the maps μ_k.

Certainly, not all elements of $\mathbb{Z}_n$ are invertible. For example, 10 doesn't have an inverse in $\mathbb{Z}_{10}$: for any $\alpha \in \mathbb{Z}_{10}$, $10\alpha \neq 1$, since multiplying by 10 shifts to the left.

Claim. *If $n \in \mathbb{Z}$ and $(n, N) = 1$ then n has an inverse in $\mathbb{Z}_N$.*

Proof. Consider $f(x) = nx - 1$. Then $f'(x) = n$, and Hensel's Lemma applies, where a_0 is a multiplicative inverse of n in $\mathbb{Z}/N\mathbb{Z}$. □

Definition 2 (The n-adic Numbers)**.** $\mathbb{Q}_n = \{\sum_{k=m}^{\infty} d_k n^k : m \in \mathbb{Z}\}$. Addition and multiplication are defined the same way.

Observations: $\mathbb{Q} \subseteq \mathbb{Q}_n$ for any $n \in \mathbb{N}$. Call an element of $\mathbb{Q}_n$ *rational* if its in the image of $\mathbb{Q}$ inside $\mathbb{Q}_n$. Furthermore, $\mathbb{Q}_n = \mathbb{Z}_n[\frac{1}{n}]$. Also be cautious that the $\mathbb{Z}_n$ are not countable.

Claim. $\mathbb{Z}_n^{\times} = \{\alpha \in \mathbb{Z}_n : \alpha \pmod{n} \in (\mathbb{Z}/n\mathbb{Z})^{\times}\}$.

Proof. Check that Hensel's Lemma works also for $f \in \mathbb{Z}_n[x]$. Then apply the same proof as before. □

Claim. *$\alpha \in \mathbb{Q}_n$ is rational if and only if it is periodic.*

Proof. Same as for the reals (!). □

What about $\mathbb{Q}_n$? What are its invertible elements?

Claim. *$\mathbb{Z}_{10}$ has zero divisors.*

Proof. We'll find a solution for $x^2 = x$ which is not 1 or 0. Then $x(x-1) = 0$ and we found zero divisors. Of course, we employ Hensel's lemma. Define $f(x) = x^2 - x$, and then $f'(x) = 2x - 1$. Note $f(5) = 25 - 5 \equiv 0 \pmod{10}$ and $f'(5) = 9 \in (\mathbb{Z}/10\mathbb{Z})^{\times}$. This gives some $\alpha \in \mathbb{Z}_{10}$ whose first digit (on the right) is 5, so it's not 1 or 0, and we're done. □

This occurs only because 10 is not prime, so we can take non-trivial elements of $(\mathbb{Z}/10\mathbb{Z})^{\times}$.

Theorem 1. *Let p be prime. Then $\mathbb{Q}_p$ is a field.*

This uses the fact $\mathbb{Z}_p^{\times} = \mathbb{Z}_p \setminus p\mathbb{Z}_p$.

Exercise. *Let p be prime, m an integer. Show $\mathbb{Q}_{p^m} \cong \mathbb{Q}_p$ as rings.*

Exercise. *Show that the ring $\mathbb{R}_p = \{\pm \sum_{i=-\infty}^{n} d_i p^i : 0 \leq d_i < p, n \in \mathbb{Z}\}$, defined "the other way around" but with the same addition and multiplication, is isomorphic to $\mathbb{R}$.*

Claim. *$\mathbb{Q}_m \cong \mathbb{Q}_n$ as rings if and only if m, n have the same prime divisors.*

We somewhat waved our hands earlier, when we said addition and multiplication is defined "as usual". We give a more formal definition (practically as an inverse limit).

Definition 3 (Formal Definition of p-adic Integers)**.** Write $\mathbb{Z}_p = \{(a_i)_{i=1}^{\infty} : \forall i, a_{i+1} \equiv a_i \pmod{p^i}\}$ as a subset of the product $\prod_{i=1}^{\infty} \mathbb{Z}/p^i\mathbb{Z}$. Then, addition and multiplication are defined pointwise: $(\vec{a} + \vec{b})_i = a_i + b_i$, where the latter operation is in the appropriate ring in the product; multiplication is the same.

It is now easy to prove, formally, that $\mathbb{Z}_p$ is a ring, e.g. $((a+b)+c)_i = a_i + b_i + c_i = (a+(b+c))_i$ where the central expression is evaluated in $\mathbb{Z}/p^i\mathbb{Z}$, wherein addition is associative. We still need to convince ourselves this ring is indeed the same $\mathbb{Z}_p$ defined earlier, and this is done by mapping $\alpha = \sum_{i=0}^{\infty} d_i p^i$ in the old $\mathbb{Z}_p$ to $(\sum_{k=0}^{i-1} d_k p^k)_{i=1}^{\infty} \in \prod_{i=1}^{\infty} \mathbb{Z}/p^i\mathbb{Z}$.

Example 3. In $\mathbb{Z}_p$, we have $-1 = (p-1, p^2-1, p^3-1, \ldots)$. Generally, $(-a)_i = -a_i$ and $\left(\frac{1}{a}\right)_i = \frac{1}{a_i}$ (for $a \in \mathbb{Z}_p^{\times}$).

Definition 4 (Formal Definition of p-adic Numbers)**.** For p prime, $\mathbb{Q}_p = \mathcal{F}(\mathbb{Z}_p)$, where $\mathcal{F}(R)$ denotes the fraction field of R

For this definition, we need to show $\mathbb{Z}_p$ is a domain, i.e. that there are no zero divisors. Indeed, if $d_n, d'_m \neq 0$ then:

$$\left(\sum_{i=1}^{\infty} d_i p^i\right) \cdot \left(\sum_{i=m}^{\infty} d'_i p^i\right) = (d_i d'_i \pmod p) p^{n+m} + \sum_{i=m+n+1}^{\infty} D_i p^i$$

That is to say, the first digit cannot be 0.

Theorem 2. $\mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}]$.

Proof. The inclusion $\supseteq$ is obvious. For the other direction, observe every non-zero $\alpha \in \mathbb{Z}_p$ can be written (uniquely) as $\alpha = p^n u$ where $n \in \mathbb{N}$ and $u \in \mathbb{Z}_p^{\times}$. This n is called the p-adic valuation of α; we define it in $\mathbb{Q}_p$:

$$\operatorname{val}_p\left(\sum_{i=n}^{\infty} d_i p^i, d_n \neq 0\right) = n$$

Now, for $\frac{\alpha}{\beta} \in \mathcal{F}(\mathbb{Z}_p)$, write $\beta = p^{\operatorname{val}_p(\beta)} u$, where $u = \frac{\beta}{p^{\operatorname{val}_p(\beta)}} \in \mathbb{Z}_p$, and then:

$$\frac{\alpha}{\beta} = \frac{\alpha}{p^{\operatorname{val}_p(\beta)} u} = \frac{\alpha u^{-1}}{p^{\operatorname{val}_p(\beta)}} \in \mathbb{Z}_p\left[\frac{1}{p}\right]$$

□

Example 4. In $\mathbb{Q}_5$, $\operatorname{val}_5(25) = 2$, since $25 = 0 \cdot 5^0 + 0 \cdot 5^1 + 1 \cdot 5^2$. Similarly, $\operatorname{val}_5(\frac{1}{25}) = -2$.

Claim. *The map $\operatorname{val}_p : \mathbb{Q}_p^{\times} \to \mathbb{Z}$ is a homomorphism. This only works when p is prime.*

Note we define $\operatorname{val}_p(0) = \infty$.

Claim. *For any $\alpha, \beta \in \mathbb{Q}_p$, $\operatorname{val}_p(\alpha + \beta) \geq \min\{\operatorname{val}_p(\alpha), \operatorname{val}_p(\beta)\}$.*

Claim. $p\,\mathbb{Z}_p = \{\sum_{i=1}^{\infty} d_i p^i\} = \{\alpha : \operatorname{val}_p(\alpha) \geq 1\} \lhd \mathbb{Z}_p$ *is a maximal ideal.*

Proof. That it is an ideal is easy from the second presentation given. That it is maximal follows from $\alpha \notin p\,\mathbb{Z}_p \iff \alpha \in \mathbb{Z}_p^{\times}$. Another proof is that $\mathbb{Z}_p / p\,\mathbb{Z}_p \cong \mathbb{F}_p$ by the first isomorphism theorem with the map $\mathbb{Z}_p \xrightarrow{\bmod p} \mathbb{F}_p$. □

Claim. *The ideal $p\,\mathbb{Z}_p$ is a unique maximal ideal in $\mathbb{Z}_p$. In fact, any ideal in $\mathbb{Z}_p$ is of the form $p^n\,\mathbb{Z}_p$.*

Proof. The first statement follows from the fact that in a domain R, the non-units form an ideal if and only if there is a unique maximal ideal. We show the second statement. Let $I \lhd \mathbb{Z}_p$ and $n = \min\{\operatorname{val}_p(\alpha) : \alpha \in I\}$. We claim $I = p^n\,\mathbb{Z}_p$. We know there exists $\alpha \in I$ with $\operatorname{val}_p(\alpha) = n$, so $p^n\,\mathbb{Z}_p = p^n u\,\mathbb{Z}_p = \alpha\,\mathbb{Z}_p \subseteq I$, where $\alpha = p^n u$. In the other direction, $I \subseteq p^n\,\mathbb{Z}_p$ for otherwise there exists $\alpha \in I$ with $\operatorname{val}_p(\alpha) < n$. □

Claim. $\mathbb{Q}_p^{\times} \cong \mathbb{Z} \times \mathbb{Z}_p^{\times}$ *via* $\alpha \xrightarrow{\psi} \left(\operatorname{val}_p(\alpha), \frac{\alpha}{p^{\operatorname{val}_p(\alpha)}}\right)$.

This has some applications, e.g. that $\alpha \in \mathbb{Q}_p^{\times}$ is a square if and only if $\operatorname{val}_p(\alpha) \in 2\,\mathbb{Z}$ and $\frac{\alpha}{p^{\operatorname{val}_p(\alpha)}}$ is a square in $\mathbb{Z}_p$. Indeed, $\beta^2 = \alpha$ gives $\psi(\beta)^2 = \psi(\alpha)$, but $\psi(\beta)^2 = \left(2\operatorname{val}_p(\beta), \left(\frac{\beta}{p^{\operatorname{val}_p(\beta)}}\right)^2\right) = \left(\operatorname{val}_p(\alpha), \frac{\alpha}{p^{\operatorname{val}_p(\alpha)}}\right)$.

Claim. *Let $r \in \mathbb{Q}^{\times}$. Then $x^2 = r$ is solvable in $\mathbb{Q}$ if and only if it is solvable in $\mathbb{R}$ and every $\mathbb{Q}_p$.*

Proof. One direction is easy. Assume $x^2 = r$ is solvable in $\mathbb{R}$ and in every $\mathbb{Q}_p$. Because it is solvable over the reals, $r > 0$. Since it is solvable in $\mathbb{Q}_p$, $\operatorname{val}_p(r) \in 2\,\mathbb{Z}$. Observe that for $r \in \mathbb{Q}^{\times}$, $\operatorname{val}_p(r) = n$ such that $r = p^n \frac{a}{b}$ with $p \nmid a, b$ and $n \in \mathbb{Z}$. Write $r = \pm \prod p_i^{e_i}$ with $e_i \in \mathbb{Z}$. But from what we just saw, $r = +\prod p_i^{e_i}$ and $e_i \in 2\,\mathbb{Z}$. This means $\sqrt{r} = \prod p_i^{e_i/2} \in \mathbb{Q}$. □

Theorem 3 (Hasse-Minkowski)**.** *A homogenous, quadratic polynomial (in many variables) has a non-trivial solution in $\mathbb{Q}$ if and only if it has a non-trivial solution in $\mathbb{R}$ and in every $\mathbb{Q}_p$.*

Exercise. *Every real number is a square up to a choice of ±. Show that in the p-adics, in a similar sense:*

$$[\mathbb{Q}_p^\times : \mathbb{Q}_p^{\times 2}] = \begin{cases} 4 & p \neq 2 \\ 8 & p = 2 \end{cases}$$

2 Topology on $\mathbb{Q}_p$

We want $\left(\sum_{i=n}^{N} d_i p^i\right)_{N=n}^{\infty}$ to be Cauchy with limit $\sum_{i=n}^{\infty} d_i p^i$.

Definition 5 (The p-adic Norm on $\mathbb{Q}$)**.** For $r \in \mathbb{Q}$, $|r|_p = p^{-\operatorname{val}_p(r)}$. In other words, $|p^n \cdot \frac{a}{b}|_p = p^{-n}$ where $p \nmid a, b$.

Example 5. $|1|_5 = 1, |5|_5 = \frac{1}{5}, |100|_5 = \frac{1}{25}$, $|500|_5 = \frac{1}{125}$. $|\frac{3}{25} + \frac{1}{5}|_5 = 25$.

Definition 6 (p-adic Distance on $\mathbb{Q}$)**.** Define $\operatorname{dist}_p(r, r') = |r - r'|_p$.

Theorem 4. *$\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to* dist_p.

Proof. Recall the completion is defined as a quotient space of the set of Cauchy sequences. We map $\mathbb{Q}_p$ to the completion of $\mathbb{Q}$ with respect to dist_p, via $\sum_{i=n}^{\infty} d_i p^i \mapsto (\sum_{i=n}^{N} d_i p^i)_{N=n}^{\infty}$. We leave it as an exercise to verify this is a bijective homomorphism. Alternatively, note that $(\mathbb{Q}_p, \operatorname{dist}_p)$ is complete, and $\mathbb{Q}$ is dense in it. □

This allows us to 'start our story' with $\mathbb{Q}$ and define $\mathbb{Q}_p$ as in the theorem above. Just to recapitulate, in $\mathbb{Q}$ we define the p-adic norm as $|p^n \cdot \frac{a}{b}|_p = p^{-n}$ (where $p \nmid a, b$) and in $\mathbb{Q}_p$ we define $|\sum_{i=n}^{\infty} d_i p^i| = p^{-n}$ (where $d_n \neq 0$).

We want $\mathbb{Q}_p$ to be defined by the topology defined by the prebasis $\{p^n \mathbb{Z}_p : n \in \mathbb{Z}\} = \{\operatorname{val}_p^{-1}([n, \infty))\}$, and this is indeed the case; a Cauchy sequence has a tail containing these.

Theorem 5 (Haar Measure)**.** *If G is a locally compact topological group, there exists a (unique up to scaling) regular, Borel, left-invariant measure on G.*

We hesitantly explain the terminology used here. A *measure* on S is a way of assigning a 'volume' to subsets of S, $\mu : X \to \mathbb{R}_{\geq 0}$ where $X \subseteq \mathcal{P}(S)$, such that μ is σ-additive; the measure of the union of countably many disjoint sets is the sum of the measures. Not all subsets of S need be measurable, and there are constraints on X which we do not mention here. A measure is *left-invariant* if $\mu(gA) = \mu(A)$ for every $g \in G, A \subseteq G$. A measure if *regular* if when $A = \bigcap A_n$ where $A_n \supseteq A_{n+1}$ and these are all open, $\mu(A) = \lim \mu(A_n)$; we also require the same is true when $A = \bigcup A_n$, $A_n \subseteq A_{n+1}$ and these are compact. *Borel* means all open sets are measurable.

Example 6. The simple examples are $\mathbb{R}^+$ with $\mu([a, b]) = b - a$ and $\mathbb{R}_{>0}^\times$ with $\mu([a, b]) = \log \frac{b}{a}$.

Recall $\{p^n \mathbb{Z}_p : n \in \mathbb{Z}\}$ is a basis for the topology of $\mathbb{Q}_p$. We show each of the $p^n \mathbb{Z}_p$ is compact. Start with $\mathbb{Z}_p$. Recall it comprises of 'compatible' sequences in $\prod_{i=1}^{\infty} (\mathbb{Z} / p^i \mathbb{Z})$. It can be shown that the product topology is compatible with the topology we have already defined. We need to show the set of compatible sequences is closed in it, and then it is also compact; this is done by noting each non-compatible sequence has a neighborhood of non-compatible sequences (we can change anything we want after the 'incompatible point'). This is a messy argument, a more intuitive explanation that $\mathbb{Z}_p$ is compact is that it comprises of sequences of digits on the left of the decimal point; this is essentially the same as taking sequences on the right of the decimal point, which is the set $[0, 1]$ in $\mathbb{R}$, which is compact - a bit more formally, we can show it is sequentially compact via a 'diagonal element'. A third argument is that $\mathbb{Z}_p = B_0(1) \subseteq \mathbb{Q}_p$ in dist_p. In any case, we have that $\mathbb{Z}_p$ is compact, and then $p^n \mathbb{Z}_p$ is compact as $\mathbb{Q}_p^\times$ acts on $(\mathbb{Q}_p, +)$ by homeomorphisms (prove this!). Another argument is that $p^n \mathbb{Z}_p = B_0(p^{-n})$. We conclude $\mathbb{Q}_p$ is locally compact (as it has a basis of compact subsets).

The following definition follows from Haar's theorem.

Definition 7. Define μ_p to be the unique Haar measure on $(\mathbb{Q}_p, +)$ such that $\mu_p(\mathbb{Z}_p) = 1$. When p is clear, we'll write μ for short.

Example 7. $\mu_p(p\,\mathbb{Z}_p) = \frac{1}{p}$. $\mu_p(\mathbb{Z}_p^\times) = \frac{p-1}{p}$.

Proof. This is due to the fact $\mathbb{Z}_p = \bigsqcup_{i=0}^{p-1}(i + p\,\mathbb{Z}_p)$, and then $1 = \mu(\mathbb{Z}_p) = \sum_{i=0}^{p-1} \mu(i + p\,\mathbb{Z}_p) = p\mu(p\,\mathbb{Z}_p)$. The second claim follows. □

Now note that the absolute value of a number tells us 'how much it stretches sets': $|a| = \frac{\mu_{\text{Eucl}}(aA)}{\mu_{\text{Eucl}}(A)}$. This is also true of the p-adic measure: $|\alpha|_p = \frac{\mu_p(\alpha A)}{\mu_p(A)}$.

We now recap our intuition and reasoning, for our own sanity and clarity.

We want $\sum^N d_i p^i$ to converge to $\sum^\infty d_i p^i$. This gives sequential compactness of $\mathbb{Z}_p$. Let us pretend we already know $\mathbb{Z}_p$ is in fact compact. This implies that $\mathbb{Z}_p$ has finite volume under a Haar measure on $(\mathbb{Q}_p, +)$, so we normalize it to be $\mu_p(\mathbb{Z}_p) = 1$. This allows us to alternatively define $|\alpha|_p$ by $\mu_p(\alpha S) = |\alpha|_p \mu_p(S)$, with any $S \subseteq \mathbb{Q}_p$ Borel. Note it needs to be shown that such a number is well-defined for any α, i.e. that the ratio is independent of S. To show this, one can show any such open or compact S can be written as a union of translations and scalings of $\mathbb{Z}_p$. If $|\alpha|_p$ is well-defined, any S with $\mu(S) \neq 0$ gives $|\alpha|_p = \frac{\mu_p(\alpha S)}{\mu_p(S)}$. Now take $S = \mathbb{Z}_p$. If $u \in \mathbb{Z}_p^\times$, we get $|u|_p = \frac{\mu(u\,\mathbb{Z}_p)}{\mu_p(\mathbb{Z}_p)} = \frac{\mu_p(\mathbb{Z}_p)}{\mu_p(\mathbb{Z}_p)} = 1$, and $|p|_p = \frac{\mu(p\,\mathbb{Z}_p)}{1} = \frac{1}{p}$. In general, $\alpha \in \mathbb{Q}_p^\times$ can be written as $\alpha = p^m u$ with $u \in \mathbb{Z}_p^\times, m \in \mathbb{Z}$, and then $|\alpha|_p = \frac{1}{p^m} = p^{-\operatorname{val}_p(\alpha)}$. We need to show this is indeed an absolute value on $\mathbb{Q}_p$, that is, that $|\alpha| = 0$ if and only if $\alpha = 0$, that $|\alpha\beta| = |\alpha||\beta|$ and that $|\alpha + \beta| \leq |\alpha| + |\beta|$.

Claim. *If F is a topological field with a Haar measure μ and $|\cdot| : F \to \mathbb{R}_{\geq 0}$ satisfies $|\alpha| = \frac{\mu(\alpha S)}{\mu(S)}$ for all $S \subseteq F$, then $|\cdot|$ is a norm.*

Proof. Indeed, multiplicativity follows from $|\alpha\beta| = \frac{\mu(\alpha\beta S)}{\mu(S)} = \frac{\mu(\alpha\beta S)}{\mu(\beta S)} \frac{\mu(\beta S)}{\mu(S)} = |\alpha||\beta|$. Sub-additivity follows from $|\alpha + \beta| = \frac{\mu((\alpha+\beta)S}{\mu(S)} = \frac{\mu(\alpha S + \beta S)}{\mu(S)} \leq \frac{\mu(\alpha S) + \mu(\beta S)}{\mu(S)} = |\alpha| + |\beta|$. We leave positivity to the reader. □

These properties can also be checked directly for our $|\cdot|_p$. This norm now allows us to define a metric on $\mathbb{Q}_p$ by $\operatorname{dist}_p(\alpha, \beta) = |\alpha - \beta|_p$.

Now note $|\cdot|_p|_{\mathbb{Q}}$ is an absolute value on $\mathbb{Q}$ given by $|p^m a/b| = p^{-m}$ when $p \nmid a, b$.

Theorem 6. *$\mathbb{Q}$ is dense in $\mathbb{Q}_p$ with respect to dist_p and $\mathbb{Z}$ is dense in $\mathbb{Z}_p$.*

Proof. We start with the claim for $\mathbb{Z} \subseteq \mathbb{Z}_p$. We need to show that if $\emptyset \neq U \subseteq \mathbb{Z}_p$ is open then there exists an integer $m \in \mathbb{Z}$ in U. Let $\varepsilon > 0$ and $\alpha \in \mathbb{Q}_p$ be such that $B_\varepsilon(\alpha) \subseteq U$. Let $m \in \mathbb{Z}$ be such that $p^{-m} < \varepsilon$, and take $n = \alpha \pmod{p^m}$. Then $\operatorname{dist}_p(n, \alpha) \leq p^{-m} < \varepsilon$, since they agree on the first m digits. Thus $n \in B_\varepsilon(\alpha) \subseteq U$, as desired. For $\mathbb{Q} \subseteq \mathbb{Q}_p$, the proof is the same, where the modulo maps $\sum_{j=N}^\infty d_i p^i$ to $\sum_{j=N}^{m-1} d_i p^i$, which is rational. In fact, this even shows $\mathbb{Z}[\frac{1}{p}] = \{\frac{a}{p^m} : a, m \in \mathbb{Z}\}$ is dense in $\mathbb{Q}_p$. □

It follows $\mathbb{Q}_p$ is the metric completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.

Recall two norms are called *equivalent* if one is a power of the other.

Theorem 7 (Ostrowski)**.** *Up to equivalence, every absolute value on $\mathbb{Q}$ is either $|\cdot|_{\mathbb{R}}$ or $|\cdot|_p$ for some prime p.*

We note Ostrowski's theorem generalizes to number fields, i.e. finite extensions of $\mathbb{Q}$. For example, the only absolute values on $\mathbb{Q}(i)$ are $|a + bi| = \sqrt{a^2 + b^2}$ and $|\alpha|_\pi = |\,\mathbb{Z}[i]/\pi|^{-\operatorname{val}_\pi(\alpha)}$ for π a prime in $\mathbb{Z}[i]$, which are precisely $1 + i$, primes p with $p \equiv 3 \pmod 4$ and 2 factors of every $p \equiv 1 \pmod 4$ (which split over $\mathbb{Q}(i)$, e.g. $13 = (3 + 2i)(3 - 2i)$).

3 Dual Groups

Definition 8. Let G be a topological, locally compact, abelian group. The *dual group* $\hat{G}$ is defined as the set of topological group homomorphisms from G to $S^1 = \{z \in \mathbb{C} : |z| = 1\}$, i.e. $\hat{G} = \mathrm{Hom}_{\mathrm{TopGrp}}(G, S^1)$. $\hat{G}$ is a group with respect to pointwise multiplication, and elements of it are called *characters*. If $G \cong \hat{G}$, G is called *self-dual*.

Example 8. We have $\widehat{\mathbb{Z}/n} = \{\chi_i : 1 \mapsto \zeta_n^j : j = 0, \dots, n-1\}$ with $\zeta_n = e^{\frac{2\pi i}{n}}$. It is isomorphic to $\mathbb{Z}/n$, as $\chi_j\chi_k = \chi_{j+k}$. This isomorphism is 'not canonical', as we chose a 'special' root of unity.

Example 9. $\hat{\mathbb{Z}} \cong S^1$, as in general $\mathrm{Hom}(\mathbb{Z}, G) \cong G$. $\widehat{S^1} \cong \mathbb{Z}$ as the characters are $\chi(\alpha) = \alpha^m$ for integer m (prove there are no more homomorphisms!).

Theorem 8 (Pontryagin Duality)**.** *For any topological, locally compact, abelian group G, $\hat{\hat{G}} \cong G$.*

Example 10. Take $G = \mathbb{R}$. We claim it is self-dual. We have the characters $\chi_{\infty,\beta}(\alpha) = e^{i\beta\alpha}$, and it can be shown the map $\beta \mapsto \chi_{\infty,\beta}$ gives an isomorphism $\mathbb{R} \cong \hat{\mathbb{R}}$. The only non-trivial part is showing this map is surjective, and this is a standard exercise in calculus and ODE's.

We give some intuition for defining the dual group. Take the group $\mathbb{Z}/n$, and consider the characters χ_j given by $\chi_j(1) = \zeta_n^j$. These $\{\chi_0, \dots, \chi_{n-1}\}$ form an orthonormal basis of $L^2(\mathbb{Z}/n)$. Another orthonormal basis for this space is the trivial $\{\delta_j : j = 0, \dots, n-1\}$. The change of bases between these two is called the *Fourier transform*. This can also be done for $f : S^1 \to \mathbb{C}$, wherein $f(x) = \sum_{n\in\mathbb{Z}} \alpha_n x^n$ is transformed to $\sum_{n\in\mathbb{Z}} \alpha_n \chi_n$. In general, we'd like $\hat{G}$ to be to be a orthonormal basis for $L^2(G)$. Is $\hat{\mathbb{R}} = \{\chi_{\infty,\beta}\}$ an orthonormal basis for $L^2(\mathbb{R})$? Eventually, for nice enough functions - yes; but this is complicated.

For $f \in \mathbb{C}^G$, denote by $\hat{f} : \hat{G} \to \mathbb{C}$ the function given by $f = \sum_\chi \hat{f}(\chi)\chi$. Define the *convolution* of $f, g \in \mathbb{C}^G$ by $(f * g)(x) = \sum_{y\in G} f(y)g(y^{-1}x) = \sum_{yz=x} f(y)g(z)$ (and replace the sum by an integral if the group is not discrete). The most useful property of $\hat{G}$ is that $\widehat{f * g} = \hat{f} \cdot \hat{g} : \chi \mapsto \hat{f}(\chi) \cdot \hat{g}(\chi)$.

Claim. *$\mathbb{Q}_p$ is self-dual.*

Proof. We begin with constructing a non-trivial character $\chi : \mathbb{Q}_p \to S^1$. We have $\chi(0) = 1$, and we start with the assumption $\chi(1) = 1$. This gives:

$$1 = \chi(1) = \chi\left(p \cdot \frac{1}{p}\right) = \chi\left(\frac{1}{p}\right)^p$$

Which means $\chi\left(\frac{1}{p}\right) \in \mu_p$. Now assume $\chi\left(\frac{1}{p}\right) = e^{\frac{2\pi i}{p}} = \zeta_p$. The same argument with $\frac{1}{p} = p \cdot \frac{1}{p^2}$ shows $\chi\left(\frac{1}{p^2}\right) = \sqrt[p]{\zeta_p}$, thus $\chi\left(\frac{1}{p^2}\right) \in \zeta_{p^2}\mu_p$. Assume $\chi\left(\frac{1}{p^2}\right) = \zeta_{p^2}$. Continue this way, letting $\chi\left(\frac{1}{p^n}\right) = \zeta_{p^n} = e^{\frac{2\pi i}{p^n}}$. Since $\overline{\langle\{\frac{1}{p^n} : n \in \mathbb{N}\}\rangle} = \mathbb{Q}_p$, we are almost done in constructing a non-trivial character. It remains showing it is well-defined. First of all, because 1 generates $\mathbb{Z}$, we have $\chi(\mathbb{Z}) \equiv 1$. By continuity, this gives $\chi(\mathbb{Z}_p) \equiv 1$. Take $\alpha = \sum_{j=m=\mathrm{val}_p(\alpha)}^{\infty} d_j p^j$. Then:

$$\chi(\alpha) = \chi\left(\sum_{j=m}^{-1} d_j p^j\right) \cdot \underbrace{\cancelto{1}{\chi\left(\sum_{j=0}^{\infty} d_j p^j\right)}}_{\in\mathbb{Z}_p} =$$

$$\prod_{j=1}^{|m|} \chi(p^{-j})^{d_{-j}} = \prod_{j=1}^{|m|} e^{\frac{2\pi i}{p^j} d_{-j}} = e^{2\pi i \sum_{j=1}^{|m|} d_{-j} p^{-j}} = e^{2\pi i(\alpha \mod 1)} = e^{2\pi i\alpha}$$

Where $\alpha \mod 1 = \sum_{j=\mathrm{val}(\alpha)}^{-1} d_j p^j$. This thus defines an element of $\widehat{\mathbb{Q}_p}$, which we denote $\chi_{p,1} : \mathbb{Q}_p \to S^1$, given by $\chi_{p,1}(\alpha) = e^{2\pi i\alpha}$. For any other $\beta \in \mathbb{Q}_p$, we now define $\chi_{p,\beta} = e^{2\pi i\beta\alpha} \in \widehat{\mathbb{Q}_p}$. This now makes sense of exponentiation in $\mathbb{Q}_p$, perhaps best interpreted as $e^{2\pi i(\alpha \mod 1)}$, as this is truly a rational exponent. It remains showing the map $\mathbb{Q}_p \to \widehat{\mathbb{Q}_p}$ given by $\beta \mapsto \chi_{p,\beta}$ is an isomorphism. It can be seen this is a homomorphism, and it is injective as it has no kernel. We show it is surjective. Let $1 \neq \chi \in \widehat{\mathbb{Q}_p}$. We want to show $\chi = \chi_{p,\beta}$ for some $\beta \in \mathbb{Q}_p$. Since $\chi(0) = 1$ and χ is continuous, some neighborhood $p^m\,\mathbb{Z}_p$ satisfies $\chi(p^m\,\mathbb{Z}_p) \subseteq B_{\frac{1}{4}}(1)$. Since $p^m\,\mathbb{Z}_p$ is a subgroup of $\mathbb{Q}_p$, its image $\chi(p^m\,\mathbb{Z}_p)$ is a subgroup of S^1. But since its also contained in $B_{\frac{1}{4}}(1) \cap S^1$, it must be trivial: $\chi(p^m\,\mathbb{Z}_p) = 1$. Take a minimal such m, i.e, m with $\chi|_{p^m\,\mathbb{Z}_p} \equiv 1$ and $\chi|_{p^{m-1}\,\mathbb{Z}_p} \not\equiv 1$. But now $\tilde{\chi}(\alpha) = \chi(p^m\alpha)$ satisfies $\tilde{\chi}|_{\mathbb{Z}_p} \equiv 1$ and $\tilde{\chi}|_{p^{-1}\,\mathbb{Z}_p} \not\equiv 1$, so that $\tilde{\chi}\left(\frac{1}{p}\right) \neq 1$. We know $\tilde{\chi}\left(\frac{1}{p}\right) = \zeta_p^{d_0}$ for $1 \leq d_0 \leq p-1$. Continuing as we did earlier, it can be seen that $\tilde{\chi}\left(\frac{1}{p^2}\right)$ must be a p'th root of $\zeta_p^{d_0}$, and these are necessarily of the form $\zeta_{p^2}^{pd_1+d_0}$ with $0 \leq d_1 \leq p-1$. Continuing this way, we have $\tilde{\chi}\left(\frac{1}{p^n}\right) = \zeta_{p^n}^{p^{n-1}d_{n-1}+p^{n-2}d_{n-2}+\cdots+d_0}$. Consider $\beta = \sum_{i=0}^{\infty} d_i p^i$. Since $d_0 \neq 0$, this is an element of $\mathbb{Z}_p^\times$. Now notice:

$$\chi_{p,\beta}\left(\frac{1}{p}\right) = e^{2\pi i\beta\frac{1}{p}} = \zeta_p^\beta = \zeta_p^{d_0}$$
$$\chi_{p,\beta}\left(\frac{1}{p^2}\right) = e^{2\pi i\beta\frac{1}{p^2}} = \zeta_{p^2}^\beta = \zeta_{p^2}^{pd_1+d_0}$$

And so on. Generally, $\chi_{p,\beta}\left(\frac{1}{p^n}\right) = \tilde{\chi}\left(\frac{1}{p^n}\right)$. This means $\tilde{\chi}|_{\mathbb{Z}\left[\frac{1}{p}\right]} = \chi_{p,\beta}|_{\mathbb{Z}\left[\frac{1}{p}\right]}$ and since this set is dense in $\mathbb{Q}_p$, continuity gives $\tilde{\chi} = \chi_{p,\beta}$ everywhere. We then get $\chi = \chi_{p,p^m\beta}$, as desired. □

Exercise. *What's* $\widehat{\mathbb{Z}_p}$*?*

On a completely unrelated note, notice that $\mathbb{R}^\times \cong \mathbb{R} \times \mathbb{Z}/2$ via $\alpha \mapsto (\log|\alpha|, \operatorname{sgn}\alpha)$. In a similar sense, notice $\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}_p^\times$ via $\alpha \mapsto (\mathrm{val}_p(\alpha), \alpha|\alpha|_p)$. A nice exercise is to see that even $\mathbb{Z}_p^\times$ decomposes similarly as:

$$\mathbb{Z}_p^\times = \begin{cases} \mathbb{Z}_p \times \mathbb{Z}/(p-1) & p \neq 2 \\ \mathbb{Z} \times \mathbb{Z}/2 & p = 2 \end{cases}$$

This is done via defining the p-adic exponential as $e^\alpha = \sum_{n=0}^{\infty} \frac{\alpha^n}{n!}$, and showing it converges on $p\,\mathbb{Z}_p$.

Claim. $\mathbb{Q}_p/\mathbb{Z}_p \cong \mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$. *This is called the* Prüfer Group*.*

Proof. First isomorphism theorem with $\alpha \mapsto \alpha + \mathbb{Z}_p$ for $\alpha \in \mathbb{Z}[\frac{1}{p}]$. □

Claim. *Let $H \leq G$ be abelian groups. Then $\widehat{G/H} = \left\{\chi \in \hat{G} : \chi|_H \equiv 1\right\}$.*

From this we deduce the dual group of the Prüfer group is $\left\{\chi \in \widehat{\mathbb{Q}_p} : \chi|_{\mathbb{Z}_p} \equiv 1\right\}$. But it is easy to see this is precisely $\{\chi_{p,\beta} : \beta \in \mathbb{Z}_p\}$, which is isomorphic to $\mathbb{Z}_p$. This gives another place in which the p-adics naturally occur; notice the Prüfer group is not defined as anything having to do with the p-adic numbers.

We now deviate and ask ourselves about the dual group of $\mathbb{Q}$. Firstly, we have the characters $r \overset{\chi_{\infty,\beta}}{\mapsto} e^{2\pi i\beta r}$. These seem to be all, but this is only the case if we restrict ourselves to continuity with respect to the topology on $\mathbb{Q}$ defined by the real metric. Let us now forget about any topology on $\mathbb{Q}$ (or equivalently give it the discrete topology). Now notice all the new characters we have:

$$\begin{tikzcd}
\mathbb{Q} \arrow[r] \arrow[dr] \arrow[ddr, bend right] & \mathbb{R} \arrow[r, "\chi_{\infty,\beta}"] & S^1 \\
& \mathbb{Q}_2 \arrow[ur, "\chi_{2,\beta}"'] & \\
& \mathbb{Q}_3 \arrow[uur, bend right, "\chi_{3,\beta}"'] &
\end{tikzcd}$$

Even more so - if we take $\beta_\infty \in \mathbb{R}$ and $\beta_2 \in \mathbb{Q}_2, \ldots, \beta_p \in \mathbb{Q}_p$ then we get another character:

$$(\chi_{\infty,\beta_\infty}\chi_{2,\beta_2}\cdots\chi_{p,\beta_p})(r) = \chi_{\infty,\beta_\infty}(r)\chi_{2,\beta_2}(r)\cdots\chi_{p,\beta_p}(r) = \text{"}\prod_{j=\infty}^{p} e^{2\pi i\beta_j r}\text{"} = \text{"}e^{2\pi i(\beta_\infty+\beta_2+\cdots+\beta_p)}\text{"}$$

Where the notation is abysmal albeit understandable. This gives a lot of new characters, but not all of them. What if we take $\beta_p \in \mathbb{Q}_p$ for *all* $p \leq \infty$? Write $\beta \in \prod_{p\leq\infty} \mathbb{Q}_p = \mathbb{R} \times \mathbb{Q}_2 \times \mathbb{Q}_3 \times \cdots$. We then define $\chi_{\mathbb{Q},\beta}(r) = \prod_{p\leq\infty} e^{2\pi i\beta_p r} = e^{2\pi i(\sum_{p\leq\infty}\beta_p)r}$. This is problematic, e.g. for $\beta = (0, \frac{1}{2}, \frac{1}{3}, \frac{1}{5}, \dots)$; we don't want infinite products. If there exists P such that $\beta_p \in \mathbb{Z}_p$ for all $p > P$, then all products are finite. Indeed, if $\beta_p \in \mathbb{Z}_p$ for all $p > P$ then the expression $\prod_{p\leq\infty} e^{2\pi i\beta_p r}$ has $\beta_p r \in \mathbb{Z}_p$ unless $p < P$, or p divides the denominator of r. There are only finitely many of these, so this is now well-defined. The collection of these β, $\mathbb{A} = \left\{\bigcup_P \mathbb{R} \times \prod_{p\leq P} \mathbb{Q}_p \times \prod_{P<p} \mathbb{Z}_p\right\}$, is called *the adeles*, and they form a ring. Sometimes we denote this product by $\prod'_{p\leq\infty} \mathbb{Q}_p$. Now, it is indeed true that every character of $\mathbb{Q}$ is of the form $\chi_{\mathbb{Q},\beta}$. It is also true that $\hat{\mathbb{A}} \cong \mathbb{A}$. An interesting thing to note is that while the map $\mathbb{A} \to \hat{\mathbb{Q}}$ mapping β to $\chi_{\mathbb{Q},\beta}$ is surjective, it has a kernel; if $s \in \mathbb{Q}$ and $\beta_\infty = -s, \beta_p = s$, we have $\chi_{\mathbb{Q},\beta} \equiv 1$. Indeed, if we write $\alpha \in \mathbb{Q}_p$ as $\alpha = \lfloor\alpha\rfloor_p + \{\alpha\}_p$ for $\lfloor\alpha\rfloor_p \in \mathbb{Z}_p$:

$$\chi_{\mathbb{Q},\beta}(r) = e^{-2\pi irs} e^{2\pi i(\overbrace{sr}^{\in\mathbb{Q}_2} + \overbrace{sr}^{\in\mathbb{Q}_3} + \cdots)} = e^{2\pi i(-sr + \{sr\}_2 + \{sr\}_3 + \cdots)}$$

If we show the expression in the parentheses is an integer, we'll be done. We show that for any rational r, $r - \sum_{p<\infty}\{r\}_p \in \mathbb{Z}$. This is somewhat of an equivalent to a partial fraction decomposition of r. Let q be prime. Then the expression we want takes the form $(r - \{r\}_q) - \sum_{\infty>p\neq q}\{r\}_p$. The value in the parentheses is in $\mathbb{Z}_q$ by definition, and so is the sum as $p \neq q$. Thus $r - \sum\{r\}_p$ is an element of $\mathbb{Z}_q$. This is true for all q, so it must be an integer.

We now get that $\hat{\mathbb{Q}} \cong \mathbb{A} \,/\, \mathbb{Q}$ via $\psi : \mathbb{A} \to \hat{\mathbb{Q}}$ given by $\beta \mapsto \chi_{\mathbb{Q},(-\beta_\infty,\beta_2,\dots)}$, which has kernel isomorphic to $\mathbb{Q}$.

Claim. *Let $r \in \mathbb{Q}$. Then $\prod_{p\leq\infty} |r|_p = 1$.*

Proof. Set $r = \pm\prod_{i=1}^n p_i^{e_i}$. Then $|r|_\infty = \prod^n p_i^{e_i}$ and $|r|_{p_i} = p_i^{-e_i}$. For all $i > n$ we get $|r|_{p_i} = 1$. These give the result. □

In the Haar measure of $\mathbb{A}$, we get $\mu(rA) = \mu(A)$ for any $r \in \mathbb{Q}$ and $A \subseteq \mathbb{A}$. Thus the action of $\mathbb{Q}$ on $\mathbb{A}$ preserves measures; this gives the *Tamagawa measure*.

4 Bruhat-Tits Building of PGL_2

4.1 Introductory Discussion and Definitions

We know $\mathrm{GL}_2(\mathbb{R})$ acts on $\mathbb{C}$ via the Möbius transformations $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) z = \frac{az+b}{cz+d}$. Now notice that for some $r \in \mathbb{R}$:

$$\frac{az+b}{cz+d} = r + i\frac{(ad-bc)\operatorname{Im} z}{|cz+d|^2}$$

This means that if $\det A > 0$ then A acts on the upper half plane $\mathcal{H} = \{z : \operatorname{Im} z > 0\}$. This allows us to define $\mathrm{GL}_2^+(\mathbb{R}) = \{A : \det A > 0\}$, and it acts on $\mathcal{H}$. In fact, note how scalar matrices act as the identity; this means we actually have an action of $\mathrm{PGL}_2^+(\mathbb{R})$ on $\mathcal{H}$. This group is in fact isomorphic to $\mathrm{PSL}_2(\mathbb{R})$ via rescaling so that the determinant is 1. This group acts on $\mathcal{H}$ by isometries. The three interesting examples are $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ which give $z \mapsto z + b, z \mapsto az$ and $z \mapsto -\frac{1}{z}$; translations, scalings and inversions. These also generate the group.

Claim. *This action is transitive.*

Proof. One can get from i to any z via scaling by $\operatorname{Im} z$ and translating by $\operatorname{Re} z$. As an element of PSL_2, this is given by $\left(\begin{smallmatrix} \sqrt{t} & s/\sqrt{t} \\ 0 & 1/\sqrt{t} \end{smallmatrix}\right)$ when $z = t + si$. Now we can get from any $w \in \mathcal{H}$ to i and from i to any $z \in \mathcal{H}$. □

Now recall that when G acts transitively on X, we have $X \cong G/\operatorname{Stab}_G(x_0)$ as G-sets (i.e. it preserves the action), for any x_0. We compute $\operatorname{Stab}(i)$. Assume $\frac{ai+b}{ci+d} = i$. We then get $ai + b = -c + di$, which gives $a = d$ and $b = -c$. Since $ad - bc = 1$, we get $a^2 + b^2 = 1$. Thus:

$$\operatorname{Stab}_{\mathrm{PSL}_2(\mathbb{R})}(i) = \left\{ \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} : \theta \in \mathbb{R} \right\} = \mathrm{PSO}(2) := \mathrm{SO}(2)/\{\pm I\}$$

So we conclude:

$$\mathcal{H} \cong \mathrm{PSL}_2(\mathbb{R})/\,\mathrm{PSO}_2(\mathbb{R}) \cong \mathrm{SL}_2(\mathbb{R})/\,\mathrm{SO}_2(\mathbb{R}) \cong \mathrm{PGL}_2^+(\mathbb{R})/\,\mathrm{SO}_2(\mathbb{R})$$

In general, let G be any matrix/Lie group such as $\mathrm{GL}_n, \mathrm{SL}_n, O_n, U_n$. The general object we should study is G modulo a maximal compact subgroup in G.

Example 11. Consider $O(n) \leq \mathrm{GL}_n$. It is closed as it is the set of solutions to $A^*A = I$, and it is bounded as the rows of such a matrix are unit vectors. Thus it is compact. We claim it is maximal. In general, the orthogonal group with respect to some inner product $\langle , \rangle$ is given by $O(\langle , \rangle) = \{A \in \mathrm{GL}_n(\mathbb{R}) : \langle Av, Aw \rangle = \langle v, w \rangle\}$, and these are all conjugate as if P is a change of matrix basis from the standard basis to some orthonormal basis of $\langle , \rangle$, we have $O(n) = PO(\langle , \rangle)P^{-1}$. Say $K \leq \mathrm{GL}_n^+(\mathbb{R})$ is compact. We show $K \leq PO(n)P^{-1}$ for some P (this is called the *Weyl trick*). Indeed, define the following inner product:

$$\langle v, w \rangle_K := \int_K \langle kv, kw \rangle dk$$

This is defined since integration over a compact group with respect to a Haar measure on it is well-defined. It can be shown $\langle , \rangle_K$ is indeed an inner product. It is also K-invariant, so that $\langle Av, Aw \rangle_K = \langle v, w \rangle$ for any $A \in K$. This is the same as saying $K \leq O(\langle , \rangle_K)$, so we're done. We conclude that $O(n)$ is maximal, otherwise we could conjugate it into a proper subset of itself, which is impossible because $O(n) \backslash P^{-1}O(n)P$ is open, so it must have positive Haar measure. We conclude $O(n)$ is a maximal compact subgroup of $\mathrm{GL}_n(\mathbb{R})$, and it is unique up to conjugation.

With similar techniques, one can show $\mathrm{SO}(n)$ is a maximal compact subgroup in $\mathrm{SL}_n(\mathbb{R})$ or $\mathrm{PSL}_n(\mathbb{R})$.

Definition 9. If G is a Lie group and $K \leq G$ is a maximal compact subgroup of G, the quotient G/K is called a *symmetric space* for G.

Let $\mathrm{SO}(2,1)$ be the group of matrices in $\mathrm{SL}_3(\mathbb{R})$ which preserve the form $\operatorname{diag}(1,1,-1)$, i.e. $\{A \in \mathrm{SL}_3(\mathbb{R}) : A^t \operatorname{diag}(1,1,-1)A = \operatorname{diag}(1,1,-1)\}$. It turns out $\mathrm{SO}(2,1) \cong \mathrm{SL}_2(\mathbb{R})$, and we have the following diagram:

$$\begin{tikzcd}
\mathrm{SL}_2(\mathbb{R}) \arrow[d, dash, "\cong"'] & \mathrm{SO}(2) \arrow[l, hook'] \arrow[d] \\
\mathrm{SO}(2,1) & \begin{pmatrix} \mathrm{SO}(2) & 0 \\ 0 & 1 \end{pmatrix} \arrow[l, hook']
\end{tikzcd}$$

Define the *Hyperbolic n-space* as $\mathcal{H}^n = \mathrm{SO}(n,1)/\operatorname{diag}(\mathrm{SO}(n),1)$. This is the "correct" generalization of $\mathcal{H}$, and not $\mathrm{SL}(n)/\,\mathrm{SO}(n)$ as one might expect. The case $n = 2$ gives an "accidental" isomorphism as $\mathrm{SL}(2) \cong \mathrm{SO}(2,1)$, but this is not true in general.

It turns out that, in general, $\mathrm{PGL}_n(\mathbb{R})/O(n)$ is identified with the set of inner products on $\mathbb{R}^n$, up to scaling. The identification takes $AO(n)$ to the inner product $\langle v, w \rangle_A = v^t AA^t w$. This is well-defined since if $B \in O(n)$ then $\langle v, w \rangle_{AB} = v^t (AB)(AB^t)w = v^t ABB^t Aw = v^t AA^t w = \langle v, w \rangle_A$. We leave it as an exercise to show this map is surjective (use Gram-Schmidt) and injective (use the definition of $O(n)$).

Our eventual goal will be to understand the symmetric space of $\mathrm{PGL}_n(\mathbb{Q}_p)$, but first let us gain some more motivation for defining real symmetric spaces.

There are many ways $\mathrm{SL}_2(\mathbb{R})$ acts on a vector space V over $\mathbb{C}$. Actions of a group on a vector space are called *representations* of the group. The group $\mathrm{SL}_2(\mathbb{R})$ is "very big" and complicated, but it has a compact subgroup $\mathrm{SO}(2) \cong S^1$. Representation theory tells us that if $\mathrm{SO}(2)$ acts on some vector space V then the matrix representing the action of some $g \in \mathrm{SO}(2)$ on V is diagonal with respect to some basis, and the diagonal is composed of characters $\chi_m(\theta) = \theta^m$, under the identification $\mathrm{SO}(2) \cong S^1$. In some sense related to our outlook on symmetric spaces, we can view the complicated group $\mathrm{SL}_2(\mathbb{R})$ as a sort of sum of $\mathrm{SO}(2)$ and $\mathcal{H}$. This is the theory of modular forms, and it allows us to understand the representation theory of $\mathrm{SL}_2(\mathbb{R})$ better.

Fix $G = \mathrm{GL}_2(\mathbb{Q}_p)$. We will soon show $K = \mathrm{GL}_2(\mathbb{Z}_p)$ is a maximal compact subgroup in G. Surprisingly, it will turn out the symmetric space is a regular tree.

Claim. *$\mathbb{Z}_p^\times = \mathrm{GL}_1(\mathbb{Z}_p) \leq \mathrm{GL}_1(\mathbb{Q}_p) = \mathbb{Q}_p^\times$ is a maximal compact subgroup.*

Proof. It is compact since $\mathbb{Z}_p^\times = \bigcup_{i=1}^{p-1} i + p\,\mathbb{Z}_p$, and $p\,\mathbb{Z}_p$ is compact. Let $\mathbb{Z}_p^\times \subset U \leq \mathbb{Q}_p^\times$. We will show U is not compact. Let $\alpha \in \mathbb{Q}_p^\times \setminus \mathbb{Z}_p^\times$. Then $\mathrm{val}_p(\alpha) \neq 0$. If its positive, consider α^{-1}, so that $\mathrm{val}_p(\alpha) < 0$. The sequence $(\mathrm{val}_p(\alpha^n))$ approaches $-\infty$, so $\{\alpha^n\}$ is not contained in any ball, and we're done. □

Claim. *$K = \mathrm{GL}_n(\mathbb{Z}_p) \leq \mathrm{GL}_n(\mathbb{Q}_p) = G$ is a maximal compact subgroup.*

Proof. The space $M_n(\mathbb{Z}_p) \cong \mathbb{Z}_p^{n^2}$ is compact, and $K = \det^{-1}(\mathbb{Z}_p^\times)$ (a matrix is invertible in a commutative ring if and only if its determinant is invertible in the ring) is closed in it (since $\mathbb{Z}_p^\times$ is closed), so it is compact. Set $K \subset U \leq \mathrm{GL}_n(\mathbb{Q}_p)$. If there exists some $g \in U$ with $\mathrm{val}_p(\det g) < 0$ then $\{\det u : u \in U\}$ is unbounded as before, so U is not compact. Thus $\det(u) \in \mathbb{Z}_p^\times$ for all $u \in U$. Take some $u \in U \setminus M_n(\mathbb{Z}_p)$. There exists some $u \in U$ with $u \notin \mathrm{GL}_n(\mathbb{Z}_p)$. We'll continue later, when we have more tools. □

The p-adic case is very different from the real case, as the groups $O(2)$ and $\mathrm{PGL}_2(\mathbb{Z}_p)$ are very different: the latter is open! Indeed, if $A \in \mathrm{GL}_2(\mathbb{Z}_p)$ then $A + M_2(p\,\mathbb{Z}_p) \in \mathrm{GL}_2(\mathbb{Z}_p)$, because $\det(A + pB) \equiv \det(A) \pmod{p}$. A quotient of a topological group by an open subgroup is discrete, so our symmetric space is discrete. In fact, it is even countable.

Claim. $|G/K| = \left|\mathrm{GL}_2(\mathbb{Q}_p)/\,\mathrm{GL}_2(\mathbb{Z}_p)\right| = \aleph_0$.

Proof. Say $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$. First, assume $\mathrm{val}_p(c) \geq \mathrm{val}_p(d)$ by applying $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \in K$ if needed. We now multiply by $\left(\begin{smallmatrix} 1 & 0 \\ -\frac{c}{d} & 1 \end{smallmatrix}\right) \in K$ (as $d \neq 0$ because $\mathrm{val}_p(c) \geq \mathrm{val}_p(d)$), attaining $\left(\begin{smallmatrix} * & b \\ 0 & d \end{smallmatrix}\right)$. Renaming, let this matrix take the form $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$. Write $a = p^n u, d = p^m u'$ with $u, u' \in \mathbb{Z}_p^\times$, and apply $\mathrm{diag}(u^{-1}, u'^{-1}) \in K$, so that we get (again, renaming) $\left(\begin{smallmatrix} p^n & b \\ 0 & p^m \end{smallmatrix}\right)$. Multiplying by $\left(\begin{smallmatrix} 1 & \frac{-b+(b \pmod{p^n})}{p^n} \\ 0 & 1 \end{smallmatrix}\right)$ we get $\left(\begin{smallmatrix} p^n & b \pmod{p^n} \\ 0 & p^m \end{smallmatrix}\right)$. This is allowed as the upper-right element is in $\mathbb{Z}_p^\times$. But there are $\aleph_0$ options for the matrix we got (notice that the upper-right element also has $\aleph_0$ options, not finitely many options), and we're done. □

A corollary to our proof is that for any $g \in G$, there's some element in gK of the form $\left(\begin{smallmatrix} p^m & b \\ 0 & p^n \end{smallmatrix}\right)$, with $b \in \mathbb{Z}\left[\frac{1}{p}\right]/(p^m)$ (that is, $b = \sum_{j=N}^{m-1} d_j p^j$).

Claim. *This element is unique.*

Proof. Say $r, r' \in gK$. Then $r^{-1}r' \in K$. Writing $r = \left(\begin{smallmatrix} p^m & b \\ 0 & p^n \end{smallmatrix}\right)$ and $r' = \left(\begin{smallmatrix} p^x & z \\ 0 & p^y \end{smallmatrix}\right)$, we get $r^{-1}r' = \left(\begin{smallmatrix} p^{x-m} & * \\ 0 & p^{y-n} \end{smallmatrix}\right)$. Since this is an element of K, it must be invertible, so we get that $x = m$ and $y = n$. Thus:

$$r^{-1}r' = \begin{pmatrix} 1 & (z-b)p^{-m} \\ 0 & 1 \end{pmatrix}$$

Again, since this is in K, $(z-b)p^{-m} \in \mathbb{Z}_p$, so that $z \equiv b \pmod{p^m}$. But z and b are reduced modulo p^m by our assumption, so $z = b$. □

We conclude G/K is identified with matrices of the form $\left(\begin{smallmatrix} p^m & b \\ 0 & p^n \end{smallmatrix}\right)$ with b reduced modulo p^m.

What can we say about $\mathrm{PGL}_2(\mathbb{Q}_p)$? Denote this group by G and let K by the image of the group $\mathrm{GL}_2(\mathbb{Z}_p)$ under $\mathrm{GL}_2(\mathbb{Z}_p) \hookrightarrow \mathrm{GL}_2(\mathbb{Q}_p) \twoheadrightarrow \mathrm{PGL}_2(\mathbb{Q}_p)$ (this image is isomorphic to $\mathrm{PGL}_2(\mathbb{Z}_p)$, so we may denote it this way occasionally). Continuing from the analysis of $\mathrm{GL}_2(\mathbb{Q}_p)$, any $g \in G$ has a unique $r \in gK$

which is of the form $\left(\begin{smallmatrix} p^m & b \\ 0 & p^n \end{smallmatrix}\right)$. Multiplying by $p^{-\min\{m,n,\mathrm{val}_p(b)\}}$ we get $\left(\begin{smallmatrix} p^t & u \\ 0 & p^s \end{smallmatrix}\right)$, with $p^t, p^s, u \in \mathbb{Z}$ (which is $\mathbb{Z}\left[\frac{1}{p}\right] \cap \mathbb{Z}_p$) and at least one is in $\mathbb{Z}_p^\times$, and also $u \in \{0, \dots, p^t - 1\}$. Thus we identify the symmetric space with the following set:

$$\mathcal{X}_2 = \left\{ \begin{pmatrix} p^m & b \\ 0 & p^n \end{pmatrix} \in M_2(\mathbb{Z}) : b \in \{0, \dots, p^m - 1\}, \text{either } n = 0, m = 0 \text{ or } p \nmid b \right\}$$

Note that this condition is equivalent to the gcd of the entries being 1.

Definition 10. A *lattice* in $\mathbb{R}^n$ is the $\mathbb{Z}$-span of n linearly independent vectors. Equivalently, it is a discrete subgroup of $\mathbb{R}^n$ not contained in any proper subspace.

Claim. *The space of all lattices in $\mathbb{R}^n$ is isomorphic to $\mathrm{GL}_n(\mathbb{R}) / \mathrm{GL}_n(\mathbb{Z})$.*

Proof. The result follows from the fact $\mathrm{GL}_n(\mathbb{R})$ acts transitively on the space of lattices (via change of basis matrices) and $\mathrm{Stab}(\mathbb{Z}^n) = \mathrm{GL}_n(\mathbb{Z})$. Now use the orbit-stabilizer theorem. □

Let L, L' be two lattices. Write $L \sim L'$ if $L = \alpha L'$ for some $\alpha \in \mathbb{R}^\times$. Then the space of lattices up to this equivalence is isomorphic to $\mathrm{PGL}_n(\mathbb{R}) / \mathrm{PGL}_n(\mathbb{Z})$, which is isomorphic to $\mathrm{GL}_n(\mathbb{R}) / (\mathrm{GL}_n(\mathbb{Z})\, \mathbb{R}^\times)$. Note that if we also want lattices up to isometries, we need to consider $O(n) \backslash \mathrm{GL}_n(\mathbb{R}) / \mathrm{GL}_n(\mathbb{Z})$.

A *rational lattice* is the $\mathbb{Z}$-span of a basis of $\mathbb{Q}^n$. The space of these is isomorphic $\mathrm{GL}_n(\mathbb{Q}) / \mathrm{GL}_n(\mathbb{Z})$, and we'll get back to it later.

Definition 11. A *p-lattice* is an element of $\mathrm{GL}_n\left(\mathbb{Z}\left[\frac{1}{p}\right]\right) / \mathrm{GL}_n(\mathbb{Z})$.

From now on, we only consider lattices up to scaling. Thus we wish to study $\mathrm{PGL}_n\left(\mathbb{Z}\left[\frac{1}{p}\right]\right) / \mathrm{PGL}_n(\mathbb{Z})$, and in particular find nice representatives for it.

Definition 12. Say $v_1, \dots, v_n$ are columns of $A \in \mathrm{GL}_n\left(\mathbb{Z}\left[\frac{1}{p}\right]\right)$ and L is the $\mathbb{Z}$-span of the v_i. The *covolume* is defined as $\mathrm{covol}(L) = \mathrm{vol}(\mathbb{R}^n / L) = |\det(A)|$, which is an element of $p^{\mathbb{Z}} = \{p^n : n \in \mathbb{Z}\}$.

Claim. *The space of p-lattices is identified with the space of $\mathbb{Z}$-spans of vectors in $\mathbb{Z}\left[\frac{1}{p}\right]^n$ whose covolume is a power of p.*

For any $A \in \mathrm{GL}_n(\mathbb{Z}[p^{-1}])$, there exists a unique $B \in \mathbb{Z}[p^{-1}]^\times A = p^{\mathbb{Z}} A$ such that $B \in M_n(\mathbb{Z})$ and $\frac{1}{p} B \notin M_n(\mathbb{Z})$.

Definition 13. A matrix $B \in M_n(\mathbb{Z})$ is called *p-primitive* if $|\det B| \in p^{\mathbb{N}}$ and $\frac{1}{p} B \notin M_n(\mathbb{Z})$.

Definition 14. A lattice L is called *p-primitive* if $L \leq \mathbb{Z}^n$, $\mathrm{covol}(L) \in p^{\mathbb{N}}$ and $\frac{1}{p} L \not\leq \mathbb{Z}^n$.

We have the following identifications:

$$p\text{-primitive matrices} / \mathrm{GL}_n(\mathbb{Z}) \cong p\text{-primitive lattices} \cong \mathrm{PGL}_n(\mathbb{Z}[p^{-1}]) / \mathrm{PGL}(\mathbb{Z})$$

Here are some p-primitive lattices:

$$\left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} p \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} p \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\rangle,$$

Let $L = \langle v_1, v_2 \rangle$. This is the same as the product of the matrix A whose columns are v_1, v_2 with all vectors in $\mathbb{Z}^2$. This is the same as the product of AB with vectors in $\mathbb{Z}^2$, where $B \in \mathrm{GL}_2(\mathbb{Z})$ is an elementary matrix. Thus our freedom in choosing A is up to elementary matrix. Let $L = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mathbb{Z}^2$ be p-primitive. We want a canonical representation for the action of this matrix on $\mathrm{GL}_2(\mathbb{Z})$. First, use $\mathrm{GL}_2(\mathbb{Z})$ to perform Euclid's gcd algorithm on $(c\ d)$. This gives $\left(\begin{smallmatrix} * & * \\ 0 & \gcd(c,d) \end{smallmatrix}\right) \in M_2(\mathbb{Z})$. This is an integral, upper-triangular matrix whose determinant is a power of p, so it is of the form $\left(\begin{smallmatrix} p^m & b \\ 0 & p^n \end{smallmatrix}\right)$. Now use $\left(\begin{smallmatrix} 1 & \pm 1 \\ 0 & 1 \end{smallmatrix}\right)$

to make $b \in 0, \dots, p^m - 1$. By p-primitivity, we get either $m = 0, n = 0$ or $p \nmid b$. We proved each p-primitive lattice has a basis in $\mathcal{X}_2$ (i.e. columns of a matrix in $\mathcal{X}_2$). This basis is unique; we showed that even $\mathrm{GL}_2(\mathbb{Z}_p)$ doesn't take an element of $\mathcal{X}_2$ to a different one, so $\mathrm{GL}_2(\mathbb{Z})$ doesn't as well. To summarize:

$$\mathrm{PGL}_2\left(\mathbb{Z}\left[\frac{1}{p}\right]\right) / \mathrm{PGL}_2(\mathbb{Z}) \cong p\text{-primitive lattices} \cong \mathcal{X}_2 \cong \mathrm{PGL}_2(\mathbb{Q}_p) / \mathrm{PGL}_2(\mathbb{Z}_p)$$

All of these views are useful.

4.2 The Bruhat-Tits Tree of PGL_2

We now endow $\mathcal{X}_2$ with a directed graph structure. The idea is to connect a lattice L with a sublattice $L' \leq L$ if $[L : L'] = p$, though this won't work precisely.

$$\begin{tikzcd}
& & \begin{pmatrix}1 & \\ & 1\end{pmatrix} \arrow[lld] \arrow[ld] \arrow[d] \arrow[rd] \arrow[rrd] & & \\
\begin{pmatrix}p & \\ & 1\end{pmatrix} & \begin{pmatrix}p & 1 \\ & 1\end{pmatrix} & \cdots & \begin{pmatrix}p & p-1 \\ & 1\end{pmatrix} & \begin{pmatrix}1 & \\ & p\end{pmatrix}
\end{tikzcd}$$

In general, any lattice is isomorphic to $\mathbb{Z}^2$, and if $L' \underset{p}{<} L$ then also $pL \subseteq L'$ by abstract nonsense: $0 \to L' \to L \to L/L' \cong \mathbb{Z}/p\mathbb{Z} \to 0$. Thus we look for intermediate lattices $pL < - < L$, and the fourth isomorphism theorem tells us these correspond to subgroups of $L/pL \cong \mathbb{F}_p^2$, of which there are $p+1$. The problem here is that we'll get $\left(\begin{smallmatrix}p & \\ & p\end{smallmatrix}\right)$ connected to $\left(\begin{smallmatrix}p & \\ & 1\end{smallmatrix}\right)$, which is not primitive.

Definition 15 (Bruhat-Tits Tree of PGL_2)**.** Endow $\mathcal{X}_2$ with the following graph structure. Connect L to L' whenever L' is the primitive scaling of an index p sublattice of L; that is, $L' \underset{p}{<} L$ or $pL' \underset{p}{<} L$. The neighbors of $A \in \mathcal{X}_2$ are thus:

$$A\begin{pmatrix}p & \\ & 1\end{pmatrix}, A\begin{pmatrix}p & 1 \\ & 1\end{pmatrix}, \dots, A\begin{pmatrix}p & p-1 \\ & 1\end{pmatrix}, A\begin{pmatrix}1 & \\ & p\end{pmatrix}$$

With the following two corrections:

1. Scale the matrix by p so it is primitive, if needed.
2. Reduce the upper-right element mod the upper-left element.

These edges will be called $e_0, \dots, e_{p-1}, e_\infty$, and the corresponding matrices $N_0, \dots, N_{p-1}, N_\infty$. An equivalent definition, in terms of the two quotient space presentations we gave above, is to connect gK for $g \in \mathcal{X}_2$ to $gN_0K, \dots, gN_{p-1}K, gN_\infty K$ via the edges $e_0, \dots, e_{p-1}, e_\infty$. We have to take $g \in \mathcal{X}_2$ so that the labelling of our edges is well-defined.

An example of the last correction is e_∞ which goes out from $\left(\begin{smallmatrix}p & 1 \\ & 1\end{smallmatrix}\right)$, which gives $\left(\begin{smallmatrix}p & p \\ & p\end{smallmatrix}\right)$ after multiplication, which after the first correction gives $\left(\begin{smallmatrix}1 & 1 \\ & 1\end{smallmatrix}\right)$, which is then reduced to the identity matrix, since they give the same lattice.

This choice for the geometric structure of $\mathcal{X}_2$ might seem somewhat arbitrary. We later explain why it is canonical.

We are ready to show the main theorem.

Theorem 9. *The following hold:*

1. *The graph is symmetric (undirected).*
2. *The graph is connected.*
3. *The graph is a tree.*

Ori's Proof. 1. If $A \to B$ is an edge via e_j then $B \to A$ is an edge via e_∞. Indeed:

$$A \xrightarrow{e_j} A \begin{pmatrix} p & j \\ & 1 \end{pmatrix} \xrightarrow{e_\infty} A \begin{pmatrix} p & j \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & \\ & p \end{pmatrix} = A \begin{pmatrix} p & pj \\ & p \end{pmatrix} \equiv A \begin{pmatrix} 1 & j \\ & 1 \end{pmatrix} \equiv A \begin{pmatrix} 1 & \\ & 1 \end{pmatrix} = A$$

Similarly, if $A \to B$ via e_∞ then $B \to A$ via some e_j:

$$\begin{pmatrix} p^n & b \\ & p^m \end{pmatrix} \xrightarrow{e_\infty} \begin{pmatrix} p^n & bp \\ & p^{m+1} \end{pmatrix} \equiv \begin{pmatrix} p^n & bp \pmod{p^n} \\ & p^{m+1} \end{pmatrix} \xrightarrow{e_{\text{top digit of } b}} \begin{pmatrix} p^n & b \\ & p^m \end{pmatrix}$$

We can also see symmetry by $pL < L' < L$.

2. It suffices to show that we can connect the identity to any $\left(\begin{smallmatrix} p^n & b \\ & p^m \end{smallmatrix}\right)$. Since the graph is symmetric, we can show that any $\left(\begin{smallmatrix} p^n & b \\ & p^m \end{smallmatrix}\right)$ is connected to the identity. We'll build a path of length $n + m = \mathrm{val}_p(\det g)$ to I. Notice the following edges:

$$\begin{aligned} n > 0 \quad & \begin{pmatrix} p^n & b \\ & p^m \end{pmatrix} \xrightarrow{e_\infty} \begin{pmatrix} p^{n-1} & b \\ & p^m \end{pmatrix} \\ n = 0 \quad & \begin{pmatrix} 1 & \\ & p^m \end{pmatrix} \xrightarrow{e_0} \begin{pmatrix} 1 & \\ & p^{m-1} \end{pmatrix} \end{aligned}$$

It is now clear how to construct the desired path: $e_0^m e_\infty^n$.

3. We count $\mathcal{X}_2^\ell = \{g \in \mathcal{X}_2 : \ell(g) = \ell\}$, where $\ell(g) = \mathrm{val}_p(\det g) = m + n$. We have:

$$\begin{aligned} \mathcal{X}_2^0 &= \{I\} \\ \mathcal{X}_2^1 &= \left\{ \begin{pmatrix} p & j \\ & 1 \end{pmatrix} \right\}_{j \in \mathbb{F}_p} \cup \left\{ \begin{pmatrix} 1 & \\ & p \end{pmatrix} \right\} \\ \mathcal{X}_2^2 &= \begin{pmatrix} p^2 & j \\ & 1 \end{pmatrix}_{j \in 0, \ldots, p^2 - 1} \cup \begin{pmatrix} 1 & \\ & p^2 \end{pmatrix} \cup \begin{pmatrix} p & j \\ & p \end{pmatrix}_{j \in \mathbb{F}_p^\times} \end{aligned}$$

The sizes are $1, p+1, p^2+p$. In general:

$$\mathcal{X}_2^\ell = \begin{pmatrix} p^\ell & * \\ & 1 \end{pmatrix} \cup \begin{pmatrix} p^{\ell-1} & * \\ & p \end{pmatrix} \cup \cdots \cup \begin{pmatrix} p & * \\ & p^{\ell-1} \end{pmatrix} \cup \begin{pmatrix} 1 & 0 \\ & p^\ell \end{pmatrix}$$

The number of options for each of these is $p^\ell, (p-1)p^{\ell-2}, \ldots, (p-1)p^0, 1$. Overall, we have $(p+1)p^{\ell-1}$ options. But this is the number of vertices of the ℓ'th level of a $(p+1)$-regular tree. But $\mathcal{X}_2 = \bigsqcup_{\ell=0}^\infty \mathcal{X}_2^\ell$, and for every $g \in \mathcal{X}_2^\ell$ we found a path of length ℓ from $I = \mathcal{X}_2^0$ to g. There are exactly $(p+1)p^{\ell-1}$ non-backtracking paths of length ℓ in any $(p+1)$-regular graph. Thus the paths of length ℓ achieve every $g \in \mathcal{X}_2^\ell$ once, so that $\mathcal{X}_2$ is a tree, and the ℓ we described is the level function of it.

□

We now generalize to higher dimensions. Set:

$$\begin{aligned}
\mathcal{X}_d &= \mathrm{PGL}_d(\mathbb{Q}_p)/\mathrm{PGL}_d(\mathbb{Z}_p) \cong \mathrm{PGL}_d\left(\mathbb{Z}\left[\frac{1}{p}\right]\right)/\mathrm{PGL}_d(\mathbb{Z}) \\
&\cong \left\{ \begin{pmatrix} p^{n_1} & b_{12} & \cdots & b_{1n} \\ & p^{n_2} & \cdots & \vdots \\ & & \ddots & \vdots \\ & & & p^{n_d} \end{pmatrix} : n_i, b_{ij} \in \mathbb{N}, b_{ij} \in \mathbb{Z}/p^{n_i}, \gcd = 1 \right\} \\
&\cong \{\text{primitive } p\text{-lattices in } \mathbb{Z}^d\}
\end{aligned}$$

Some of these equivalences will be in the exercise, but we now show the last one.

Assume $A \in M_d(\mathbb{Z})$ generates a primitive p-lattice $A\,\mathbb{Z}^d$. We want to show there exists a unique $B \in \mathcal{X}_d$ with $A\,\mathbb{Z}^d = B\,\mathbb{Z}^d$, which is the same as showing $B \in A \cdot \mathrm{GL}_d(\mathbb{Z})$. As before, perform Euclid's algorithm on the bottom row of A. We'll be left with a row of 0's except for the last entry, which will be the gcd of the original bottom row. Since we started with a primitive p-lattice, this last entry will be some power of p. Now perform the same algorithm on the second to last row, ignoring the last entry, above the non-zero entry of the last row. Again, we'll get zeros everywhere except on the diagonal element and the one to the right of it, and the one on the diagonal will be a power of p. Continuing this way, we'll attain an upper-triangular matrix with powers of p on the diagonal. We can now reduce all the elements above the diagonal: use $p^{n_{d-1}}$ to reduce $b_{d-1,d}$ to $0, \ldots, p^{n_{d-1}} - 1$, and continue this way for all non-diagonal elements. Uniqueness is left as an exercise.

We will define the corresponding *Bruhat-Tits Building* $\mathcal{B}_{d,p}$ later, but for now we just define the vertex set of it as $\mathcal{X}_d$. We thus have that G acts on $\mathcal{B}_{d,p}$, and the action is transitive on vertices, with the stabilizers being conjugates in G of $K = \mathrm{PGL}_d(\mathbb{Z}_p)$. We want to understand the action of K on the vertices. Start with $d = 2$. The action of some $g' \in G$ takes an edge $gK \to gN_jK$ to $g'gK \to g'gN_jK$, which is indeed an edge. It is now clear that G acts on $\mathcal{B}_2$ by graph automorphisms. Since K stabilizes the identity, its action permutes the edges connected to I. Even more so, it preserves the levels $\ell(v) = \mathrm{dist}(I, v)$, because for $k \in K$, $\ell(kv) = \mathrm{dist}(I, kv) = \mathrm{dist}(kI, kv) = \mathrm{dist}(I, v)$, where the last equality is due to the fact G acts by graph automorphisms. Another way to see this is that $\ell(kg) = \mathrm{val}_p(\det(kg)) = \mathrm{val}_p(\det k) + \mathrm{val}_p(\det g) = 0 + \mathrm{val}_p(\det g) = \mathrm{val}_p(\det g)$.

4.3 Action on the Tree

Let $H, K \leq G$ in a general group. The relation $g \sim g'$ if and only if $HgK = Hg'K$ is an equivalence relation. We can thus decompose $G = \bigsqcup_{i \in I} Hg_iK$. The Cartan decomposition finds these representatives for PGL_d.

Claim (Cartan Decomposition)**.** *Let $G = \mathrm{PGL}_d(\mathbb{Q}_p)$ and $K = \mathrm{PGL}_d(\mathbb{Z}_p)$ or $G = \mathrm{PGL}_d(\mathbb{Z}[p^{-1}])$ and $K = \mathrm{PGL}_d(\mathbb{Z})$. Then:*

$$G = \bigsqcup_{0 = n_1 \leq n_2 \leq \cdots \leq n_d} K \operatorname{diag}(p^{n_1}, \ldots, p^{n_d})K$$

Claim. *K_2 acts transitively on each level in the tree $\mathcal{B}_2$.*

Proof. Say $gK \in \mathcal{X}_2^m$. We'll show $gK \in K \operatorname{diag}(1, p^m)K$. By the Cartan decomposition, $g = k \operatorname{diag}(1, p^n)k'$ for some $k, k' \in K$. But $n = \mathrm{val}_p(\det(k \operatorname{diag}(1, p^n)k) = \mathrm{val}_p(\det g) = m$. Thus $gK = k \operatorname{diag}(1, p^m)k'K = k \operatorname{diag}(1, p^m)K$. □

Drawing this out clearly gives that $\mathcal{B}_2/K$ is a ray, with the initial point being the root of the tree (the identity), and each vertex afterwards representing some K-orbit, i.e. a sphere with respect to ℓ.

Proof of Cartan's decomposition. Let $A \in \mathrm{PGL}_d(\mathbb{Z}[p^{-1}])$. Scale A to be in $M_n(\mathbb{Z})$ and primitive, and look at the gcd of each column. Take the column with the minimal gcd, and bring it to be the first column, via actions of K from the right. Now perform Euclid's algorithm from the left on the first column, so that the first column has zeros everywhere except the top entry, which is a power of p as before. Since we picked the gcd to be minimal and the matrix is primitive, this element must be 1. Now perform column operations so that the first row also has zeros everywhere, except the top left. The matrix is now of the form $\mathrm{diag}(1, B)$ for some matrix B, which need not be primitive. Let $B = p^r B'$ for some r and primitive B'. By actions from the left and the right, we can bring B' to the form $\mathrm{diag}(1, C)$. This means that we brought the original matrix to the form $\mathrm{diag}(1, p^r, p^r C)$. Now continue this way inductively, and we'll eventually attain $G = \bigcup K \,\mathrm{diag}(p^{n_i})K$. We now show uniqueness, and we redefine $K = \mathrm{GL}_d(\mathbb{Z}), G = \mathrm{GL}_d(\mathbb{Z}[p^{-1}])$. Assume $KgK = KhK$ for $g, h \in G$ with $g, h \in M_d(\mathbb{Z})$. Then $\mathbb{Z}^d / g\,\mathbb{Z}^d \cong \mathbb{Z}^d / h\,\mathbb{Z}^d$. Indeed, write $g = k_1 h k_2$. Then:

$$\mathbb{Z}^d / g\,\mathbb{Z}^d = \mathbb{Z}^d / (k_1 h k_2\,\mathbb{Z}^d) = \mathbb{Z}^d / (k_1 h\,\mathbb{Z}^d) \underset{x \mapsto k_1^{-1} x}{\cong} \mathbb{Z}^d / h\,\mathbb{Z}^d$$

Observe that if $g = \mathrm{diag}(p^{n_1}, \ldots, p^{n_d})$ then:

$$\mathbb{Z}^d / g\,\mathbb{Z}^d = \mathbb{Z}^d / \langle (p^{n_1}, 0, \ldots, 0)^t, \ldots, (0, \ldots, 0, p^{n_d})^t \rangle \cong \mathbb{Z} / p^{n_1} \times \cdots \times \mathbb{Z} / p^{n_d}$$

Uniqueness now follows: $\prod \mathbb{Z} / p^{n_i} \cong \prod \mathbb{Z} / p^{m_i}$ if and only if $n_i = m_i$. □

This might be a good time to define a bit of notation. Let $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ be the vertex in $\mathcal{B}$ represented by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) K$.

Recall vertices in $\mathcal{B}_d$ are identified with cosets gK in G/K, and also with lattices $g\,\mathbb{Z}^d$. What are the 'Cartan spheres' of vertices in the building? In the language of cosets, they will be K-orbits, i.e. double cosets $K \backslash G / K$, and in the language of lattices, they will be isomorphism types of finite abelian groups of order p^n with $d-1$ generators; this follows from the proof above.

We now explain why our choice for edges in $\mathcal{B}_2$ is canonical. We are given the vertices $\mathcal{X}_2 = G/K$, and we want to add edges so that G acts on the resulting graph. This means that if we put some edge $\{v_0, v_1\}$ as an edge, we must add $\{gv_0, gv_1\}$ as an edge for every $g \in G$. In particular, if we connect the origin K to some gK we also have to connect K to all $v \in KgK$. But this is the sphere $S_{\ell(g)}(K)$. We can move an edge $\{K, gK\}$ around by the action of G. If $\ell(g) = 1$ then we get $\mathcal{B}_2$, since if we connect K to any element of the first sphere then it'll have to connect to every element of the first sphere, and then by translation we get our tree. If $\ell(g) \geq 2$, the resulting graph will be disconnected, since in this case we'll never be able to connect K to the first level, without creating cycles (which will "cross spheres").

We saw K acts transitively on each sphere. Consider, for example the action of K on $\mathcal{X}_2^1$. This gives a map $K \to S_{p+1}$, whose image is some transitive subgroup. Which one is it? Is our action 2-transitive? 3-transitive? $(p+1)$-transitive? A nice, relevant fact is that the only 6-transitive groups in S_n where $n \geq 6$ are A_n, S_n. In our case, consider the map $\mathrm{PGL}_2(\mathbb{Z}_p) \to \mathrm{PGL}_2(\mathbb{F}_p)$ which takes entries modulo p. This latter group acts on $\mathbb{F}_p \cup \{\infty\}$ via Möbius transformations. The point is that these are in correspondence with the edges we defined e_j for $j \in \mathbb{F}_p \cup \{\infty\}$. So, how does $\mathrm{PGL}_2(\mathbb{F}_p) \to S_{\mathbb{F}_p \cup \{\infty\}}$ look like? As we'll explain soon, together with the exercise, this action is *sharply 3-transitive*: there is a *unique* element mapping $(0, 1, \infty)$ to any (a, b, c). Looking back at our tree, this shows that for any choice of six neighbors of the $p+1$ neighbors of the identity, there is a unique element of K mapping the first to the fourth, the second to the fifth and the third to the sixth.

Definition 16 (Congruence Subgroups)**.** Define $M_d^p(\mathbb{Z}) = \mathrm{GL}_d(\mathbb{Z}[p^{-1}]) \cap M_d(\mathbb{Z}) = \{A \in M_d(\mathbb{Z}) : |\det A| \in p^{\mathbb{N}}\}$. For $\ell \geq 0$, define $K^{(\ell)} = \ker(\mathrm{GL}_d(\mathbb{Z}) \to \mathrm{GL}_d(\mathbb{Z}/p^\ell))$, the map being the modulo map.

Notice these give a filtration $\cdots \lhd K^{(2)} \lhd K^{(1)} \lhd K^{(0)} = K$, with $\bigcap K^{(\ell)} = I$.

Claim. *$K^{(\ell)}$ acts trivially on the ℓ-ball in $\mathcal{B}_2$ around $v_0 = \left[\begin{smallmatrix} 1 & \\ & 1 \end{smallmatrix}\right]$ in the building.*

Proof. Let $A \in K^{(\ell)}$. Then $A = I + p^\ell B$ for some $B \in M_d(\mathbb{Z})$. Notice that for $g = \left(\begin{smallmatrix} p^n & b \\ & p^m \end{smallmatrix}\right)$, the vertex $[g] = \left[\begin{smallmatrix} p^n & b \\ & p^m \end{smallmatrix}\right]$ is equal to gv_0. Notice $p^{n+m}\,\mathbb{Z}^2 \subseteq g\,\mathbb{Z}^2$: the former is spanned by the vectors $(p^{n+m}, 0)^t, (0, p^{n+m})^t$, and:

$$\begin{pmatrix} p^{n+m} \\ 0 \end{pmatrix} = p^m \begin{pmatrix} p^n \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 0 \\ p^{n+m} \end{pmatrix} = -b \begin{pmatrix} p^n \\ 0 \end{pmatrix} + p^n \begin{pmatrix} b \\ p^m \end{pmatrix}$$

This also implies that for any $\ell \geq m + n, p^\ell\,\mathbb{Z}^2 \subseteq g\,\mathbb{Z}^2$. Let g be with $\ell(g) \leq \ell$, i.e. in the ℓ-ball, and consider the action of A on gv_0. We have:

$$Ag\,\mathbb{Z}^2 = (I + p^\ell B)g\,\mathbb{Z}^2 \subseteq g\,\mathbb{Z}^2 + p^\ell Bg\,\mathbb{Z}^2$$

We don't know much about $Bg\,\mathbb{Z}^2$, except that it's contained in $\mathbb{Z}^2$. Thus $p^\ell Bg\,\mathbb{Z}^2 \subseteq p^\ell\,\mathbb{Z}^2 \subseteq g\,\mathbb{Z}^2$, so that overall $Ag\,\mathbb{Z}^2 \subseteq g\,\mathbb{Z}^2$. On the other hand, $A^{-1}g\,\mathbb{Z}^2 \subseteq g\,\mathbb{Z}^2$ by the same argument, as $A^{-1} \in K^{(\ell)}$. Thus $g\,\mathbb{Z}^2 \subseteq Ag\,\mathbb{Z}^2$, so that overall $Ag\,\mathbb{Z}^2 = g\,\mathbb{Z}^2$. □

We note that the other direction is also true, so that elements which act trivially on the entire ball are in $K^{(\ell)}$.

If we change our perspective to be p-adic, so that we consider the map $\mathrm{GL}_d(\mathbb{Z}_p) \to \mathrm{GL}_2(\mathbb{Z}/p^\ell)$ instead, we attain 'approximations' for elements in $\mathrm{GL}_d(\mathbb{Z}_p)$ in some sense. For $k \in \mathrm{GL}_2(\mathbb{Z}_p)$ take $k^{(\ell)} = k \pmod{p^\ell}$ (i.e. take the modulo in every entry), and these approximations get "better and better" as ℓ grows: first of all, $k^{(\ell)} \xrightarrow{\ell \to \infty} k$, but we also have $k^{-1}k^{(\ell)} \in K^{(\ell)}$, so that $k^{-1}k^{(\ell)}$ acts trivially on $B_{v_0}(\ell)$. This means k and $k^{(\ell)}$ act in the same way on $B_{v_0}(\ell)$.

We saw K acts transitively on each sphere around v_0. Does it act transitively on (infinite) rays starting from v_0? Notice that now we have to take $K = \mathrm{PGL}_2(\mathbb{Z}_p)$ and not $\mathrm{PGL}_2(\mathbb{Z})$, as the latter is countable and so does not have enough elements to act transitively. But in $\mathrm{PGL}_2(\mathbb{Z}_p)$ the answer is yes: let $v_0, v_1, \ldots$ and $v_0 = w_0, w_1, \ldots$ be two rays. Choose $k_j \in \mathrm{PGL}_2(\mathbb{Z})$ such that $k_j v_j = w_j$. Since paths from the origin are unique, $k_j v_i = w_i$ also for all $i < j$. By compactness of $\mathrm{GL}_2(\mathbb{Z}_p)$, there exists a convergent subsequence $k_{m_j} \to k_\infty \in \mathrm{GL}_2(\mathbb{Z}_p)$. It is clear k_∞ takes the ray v_i to the ray w_i: for any $\varepsilon > 0$ there exists N such that $|k_{m_j} - k_\infty| < \varepsilon$ for any $j > N$, but this means k_{m_j} and k_∞ agree on the first $f(\varepsilon)$ digits, with $f(\varepsilon) \xrightarrow{\varepsilon \to 0} \infty$. Thus k_{m_j}, k_∞ act in the same way on the $f(\varepsilon)$-ball, and we're done.

We want to study the action of the stabilizer $K = \mathrm{PGL}_2(\mathbb{Z})$ (or $\mathbb{Z}_p$) on the first sphere in the building $S = S_{v_0}(1) = \{v \in \mathcal{B}_2 : \mathrm{dist}(v, v_0) = 1\}$. Elements of this sphere correspond to sublattices of index p in $\mathbb{Z}^2$, i.e. $N_j\,\mathbb{Z}^2$ with N_j defined as before. The action is defined by the product, $k.N_j\,\mathbb{Z}^2 = kN_j\,\mathbb{Z}^2$. We saw that $K^{(1)}$ acts trivially on S, so the action factors through $K/K^{(1)}$. Recall $K^{(1)} = \ker(K \to \mathrm{PGL}_2(\mathbb{F}_p))$. But the map $\mathrm{GL}_2(\mathbb{Z}_p) \to \mathrm{GL}_2(\mathbb{F}_p)$ is surjective (by $\mathbb{F}_p \hookrightarrow \mathbb{Z}_p$). Thus $K/K^{(1)} \cong \mathrm{PGL}_2(\mathbb{F}_p)$, by $kK^{(1)} \mapsto k \pmod{p}$. The neighbors of v_0 are sublattices in $\mathbb{Z}^2$ of index p, but we saw these must contain $p\,\mathbb{Z}^2$. Hence these neighbors correspond to strictly intermediate lattices between $p\,\mathbb{Z}^2$ and $\mathbb{Z}^2$. By the correspondence theorem, these correspond to non-trivial subspaces of $\mathbb{Z}^2/p\,\mathbb{Z}^2 \cong \mathbb{F}_p^2$, i.e. lines in $\mathbb{F}_p^2$. Say $L = N_j\,\mathbb{Z}^2$. It corresponds to $\{\ell + p\,\mathbb{Z}^2\}_{\ell \in L} = L \pmod{p}$. Thus $k.L$, as a line in $\mathbb{F}_p^2$, is $kL \pmod{p}$, which is the same as $(k \mod p)(L \mod p)$. Therefore, under the identifications $K/K^{(1)} \cong \mathrm{PGL}_2(\mathbb{F}_P)$ and S with the collection of lines in $\mathbb{F}_p^2$, we got the standard action. In the exercise, you'll see this action is sharply 3-transitive.

Notice $\mathrm{Stab}_{\mathrm{Aut}(\mathcal{B}_2)}(v_0)$ acts $(p+1)$-transitively on $S_1(v_0)$, so in particular our group action doesn't realize *all* possible automorphisms of the tree. The generalization of this to higher dimensions turns out to be *false*: in $\mathcal{B}_d$, all automorphisms will come from the action of the group.

Let us now consider the action on the edges. Firstly, $g.(v, w) = (gv, gw)$. Is this transitive? This question depends on whether or not we fix orientation of the edges, but both options give interesting questions. Does G (which, recall, can be both $\mathrm{PGL}_2(\mathbb{Q}_p)$ or $\mathrm{PGL}_2(\mathbb{Z}[p^{-1}])$) take the edge $v_0 = \left[\begin{smallmatrix} 1 & \\ & 1 \end{smallmatrix}\right] \overset{e_0}{\to} \left[\begin{smallmatrix} 1 & \\ & p \end{smallmatrix}\right] = v_1$ to any $v \to w$? Since G acts transitively on the vertices, $gv = v_0$ for some $g \in G$. Since K

acts transitively on neighbors of v_0, $kgv = kv_0 = v_0$ and $kgw = v_1$ for some $k \in K$. The element kg thus gives the desired element of G.

We now find the stabilizer of an edge, $\mathrm{Stab}_G(e_0)$. It is easy to see it's the intersection $\mathrm{Stab}_G(v_0) \cap \mathrm{Stab}_G(v_1)$, but $\mathrm{Stab}_G(v_1) = \mathrm{diag}(1, p)K\,\mathrm{diag}(1, p)^{-1}$, which is the collection of $\begin{pmatrix} a & b/p \\ pc & d \end{pmatrix}$ for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in K$. The intersection is then $B := \begin{pmatrix} \mathbb{Z}_p^\times & \mathbb{Z}_p \\ p\,\mathbb{Z}_p & \mathbb{Z}_p^\times \end{pmatrix}$, as can be computed directly (this just requires writing out the definition of K). This is the preimage of the upper triangular matrices in $\mathrm{PGL}_2(\mathbb{F}_p)$, and we call it the *Iwahori* subgroup.

We denote by $\mathcal{X}_2^0$ the set of vertices of the Bruhat-Tits tree $\mathcal{X}_2$ and by $\mathcal{X}_2^1$ the set of undirected edges. We also let $\mathcal{X}_2^{\pm 1}$ be the set of directed edges in $\mathcal{X}_2$. In this notation, we saw G acts transitively on $\mathcal{X}_2^{\pm 1}$ and found its stabilizer. As an exercise, try finding the element which flips e_0, i.e. the $g \in G$ for which ge_0 is the edge $v_1 \to v_0$. In any case, one can compute:

$$\mathrm{Stab}_{\mathrm{PGL}_2(\mathbb{Z}[p^{-1}])}(e_0) = \left\{ A \in \mathrm{PGL}_2(\mathbb{Z}) : A \equiv \begin{pmatrix} * & * \\ & * \end{pmatrix} \pmod{p} \right\}$$

In $\mathrm{PGL}_2(\mathbb{F}_p)$, these $\left(\begin{smallmatrix} * & * \\ & * \end{smallmatrix}\right)$ are the stabilizers of $\infty \in \mathbb{F}_p \cup \{\infty\}$.

It is time to generalize. Define the Iwhaori subgroup in $\mathrm{PGL}_d(\mathbb{Q}_p)$ as:

$$B = \begin{pmatrix} \mathbb{Z}_p^\times & \mathbb{Z}_p & \cdots & \mathbb{Z}_p & \mathbb{Z}_p \\ p\,\mathbb{Z}_p & \mathbb{Z}_p^\times & \cdots & \cdots & \mathbb{Z}_p \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ p\,\mathbb{Z}_p & \cdots & \cdots & \mathbb{Z}_p^\times & \mathbb{Z}_p \\ p\,\mathbb{Z}_p & p\,\mathbb{Z}_p & \cdots & p\,\mathbb{Z}_p & \mathbb{Z}_p^\times \end{pmatrix}$$

This will be the pointwise stabilizer of a $(d-1)$-cell in the Bruhat-Tits building $\mathcal{X}_d$ of $\mathrm{PGL}_d(\mathbb{Q}_p)$.

Theorem 10 (Cartan Decomposition)**.** *Let $G = \mathrm{PGL}_d(\mathbb{Q}_p), K = \mathrm{PGL}_d(\mathbb{Z}_p)$. Then:*

$$G = \bigsqcup_{a \in A^+} KaK,$$

where:

$$A^+ = \{\mathrm{diag}\,(p^{m_1}, \ldots, p^{m_d}) : 0 = m_1 \leq \cdots \leq m_d\}$$

This means that $K \backslash \mathcal{X}_d^0 \cong K \backslash G / K \leftrightarrow A^+$; we'll elaborate on this later.

Let $A = \{\mathrm{diag}(p^{m_1}, \ldots, p^{m_d}) : \min\{m_i\} = 0\}$, and let S_d be the set of permutation matrices in M_d. Set $W = S_d \cdot A$ (this is a subset of the *generalized permutation matrices*). This is actually a semidirect product. This group is called the *Weyl group* (show that unlike A^+, A and W are actually groups). We can also write $W = S_d A^+ S_d$.

We now have a few decompositions, which we prove later.

Theorem 11 (Iwahori-Bruhat-Tits (?))**.**

$$G = \bigsqcup_{w \in W} BwB$$

This is to be compared to the Bruhat decomposition[2]:

Theorem 12 (Bruhat)**.** *For any field $\mathbb{F}$, let U be the subgroup of upper-triangular matrices in $\mathrm{GL}_n(\mathbb{F})$. Then:*

$$\mathrm{GL}_n(\mathbb{F}) = \bigsqcup_{\sigma \in S_n} U\sigma U$$

[2] Both of this follow from the theory of *BN-pairs*, in which a pair of subgroups of an algebraic group satisfying certain properties are given. There are two such pairs in $\mathrm{GL}_n(\mathbb{Q}_p)$, and each BN-pair gives rise to such a decomposition.

Theorem 13.

$$G = \bigsqcup_{a\in A} BaK$$

This gives the following nice result: $B\backslash\mathcal{X}_d^0 \cong B\backslash G/K \leftrightarrow A$. For $d=2$, we get $A = \{\mathrm{diag}(1,p^m)\} \cup \{\mathrm{diag}(p^m,1)\}$ and $A \cong \mathbb{Z}$ via $\mathrm{diag}(p^{m_1},p^{m_2}) \mapsto m_1 - m_2$. In PGL_d, we'll get $A \cong \mathbb{Z}^{d-1}$. The group A is identified in the building as the two-sided infinite line of diagonal matrices, and is called the *fundamental apartment* in the building.

Proof of the union part in the Iwhaori-Bruhat-Tits and BAK decomposition. It is easy to go from the BWB decomposition to the the BAK decomposition: let $g \in G$ and write $g = bwb'$ for $b, b' \in B, w \in W$. Let $w = a\sigma$ with $a \in A$ and $\sigma \in S_d$. Then $g = ba\sigma b'$ and $\sigma b' \in K$, since $B, S_d \leq K$.

Now, let us be given some $g \in \mathrm{PGL}_d(\mathbb{Q}_p)$. Acting by B from the right and left, we want to get to W. The action on the left allows us to scale a row by some invertible integral, add a $\mathbb{Z}_p$-multiple of a row to a higher row, and add a $p\,\mathbb{Z}_p$-multiple of a row to a lower row. From the right, we can scale columns by some invertible integrals, add $\mathbb{Z}_p$-multiples to "lefter" columns and $p\,\mathbb{Z}_p$-multiples to "rightier" columns. Find the minimal p-valuation of an entry of g, and take a left-bottom extremal entry g_{ij} with this valuation (so that there are no other such minimal entries on the left of that entry in the same row or below it in the same column). Using B we can ensure $g_{ij} = p^m$, and nullify the i'th row and the j'th column. Now 'forget' about this row and column, and repeat. At some point we also need to scale everything so that the minimal power is 0, and we'll end up in W. □

5 Bruhat-Tits Buildings of PGL_d

5.1 Simplicial Complexes

Recall that a graph G is simply a pair of a vertex set V together with a collection of edges $E \subseteq \binom{V}{2}$, where $\binom{X}{n}$ is the collection of (unordered) subsets of X of size n. Topologically speaking, we could think of a graph as a collection of points in space, some of which are glued together. We wish to generalize this notion to higher dimensions. There were two schools regarding this: the simplicial school and the cubic school. The former generalizes the notion of an interval to n-simplexes (triangles, tetrahedrons and so on; these are convex hulls of $n+1$ points in general position in $\mathbb{R}^n$). The latter generalizes the notion of an interval to squares, cubes, tesseracts and so on (I^n). The simplicial school won the battle of time, but there are still fields which use the advantages of the cubic school, such as geometric group theory. We can describe objects simplicialy, by describing its vertices, edges, triangles and so on.

Example 12. Take a square sheet of paper, and split it to smaller squares. Split each of these squares diagonally (say, all in the same direction). Now glue this sheet to a torus in the standard way. It is clear now what the vertices n-simplexes are, so this is a simplicial description of the torus. Note that we have to split the sheet to smaller squares, and not split it to two triangles directly, as in this way we achieve repeated edges and triangles (there is only one vertex, as we glue all the corners).

Definition 17 (Abstract Simplicial Complex)**.** An *abstract simplicial complex* is a set of vertices V together with a set of cells $X \subseteq 2^V$, such that if $\tau \subseteq \sigma \in X$ then $\tau \in X$. The *geometric realization* of the complex is the realization of the set of vertices as points in space, to which we add higher dimensional cells sequentially: connect vertices with edges, then connect edges with triangles, and so on.

5.2 Defining the Building

Let $G = \mathrm{PGL}_d(\mathbb{Q}_p)$ and $K = \mathrm{PGL}_d(\mathbb{Z}_p) = \mathrm{Stab}(\mathbb{Q}_p^\times \cdot \mathbb{Z}_p^d)$. Define $\mathcal{X}_d^0$ to be the set of $\mathbb{Q}_p^\times$-homothety classes of $\mathbb{Z}_p$-lattices in $\mathbb{Q}_p^d$. This can be identified with the quotient G/K, but also with any G/K'

for any other stabilizer K' of a lattice. Another identification is with the following set of (uniquely-determined) representatives:

$$\left\{ \begin{pmatrix} p^{n_1} & b_{12} & \cdots & b_{1n} \\ & p^{n_2} & \cdots & \vdots \\ & & \ddots & \vdots \\ & & & p^{n_d} \end{pmatrix} : n_i, b_{ij} \in \mathbb{N}, b_{ij} \in \mathbb{Z}/p^{n_i}, \gcd = 1 \right\}$$

As before, this game can be played with $G = \mathrm{PGL}_d(\mathbb{Z}[p^{-1}])$ and $K = \mathrm{PGL}(\mathbb{Z})$, etc.

The building will be a large simplicial complex. We have the vertices of the building, and now we need to decide how to construct the higher-dimensional cells. Recall we want G to act transitively on the building and K stabilizes the origin I, so that if we connect some g to I, we also have to connect kg to I for any $k \in K$. We start with connecting I to $\mathrm{diag}(1, \dots, 1, p)$. This corresponds to connecting the lattice $L_0 := \mathbb{Z}_p^d$ to $L_1 := \mathbb{Z}_p^{d-1} \times p\,\mathbb{Z}_p$. It is evident that $KL_1 = \{kL_1 : k \in K\} = \left\{ L \underset{p}{<} L_0 \right\}$, the sublattices of index p. What are these? We can put the p anywhere in the diagonal (and leave the rest as 1), and we can put anything we want above the diagonal, but only in the row where the p appears (as the elements in any other row have to be in $\mathbb{Z}/1$, which is just $\{0\}$ - it helps to think of $\mathbb{Z}/(p^i)$ as $\{0, \dots, p^i - 1\}$). This is due to the fact we can consider the index as the covolume of the lattice, which is the determinant of the matrix. In other words, $KL_1 = \{\mathrm{Span}\, B : \ell(B) = 1\}$, where $\ell(B) = \mathrm{val}_p \det B$ for $B \in \mathcal{X}_d^0$. There are thus $1 + p + \cdots + p^{d-1} = \frac{p^d - 1}{p-1}$ neighbors for the identity. This is the number of hyperplanes in $\mathbb{F}_p^d$, due to the fourth isomorphism theorem as we already analyzed above. We can now construct the edges going out of any vertex g, using the G-transitivity of the action on the building.

The same questions now persist: is this graph symmetric? is it connected?

The graph is not symmetric: we cannot, for example, connect $[\mathrm{diag}(1, \dots, 1, p)]$ back to $[I]$, as there is no scaling of the latter in which the former is of index p. However, $[\mathrm{diag}(1, \dots, 1, p)]$ will be connected to $[\mathrm{diag}(1, \dots, p, p)]$, and continuing on this way we'll get a closed loop back to $[I]$. The graph is connected: for a lattice L, scale it so that $L \subseteq \mathbb{Z}_p^d$. By Jordan-Hölder for the finite p-group $\mathbb{Z}_p^d/L$, there exists some composition series $L \underset{p}{\leq} L_{(1)} \underset{p}{\leq} L_{(2)} \underset{p}{\leq} \cdots \underset{p}{\leq} \mathbb{Z}_p^d$, so there is some path from $\mathbb{Z}_p^d$ to L. Another way is to use only $[\mathrm{diag}(p, 1, \dots, 1)], \dots, [\mathrm{diag}(1, \dots, 1, p)]$ to construct a path from L to $\mathbb{Z}_p^d$. Any edge $L_1 \to L_2$ can be completed to a cycle of length d, so we can go back.

We now describe the building of $\mathrm{PGL}_4(\mathbb{Q}_p)$. Start with $[I]$, and connect it to $[\mathrm{diag}(1, 1, 1, p)]$, then to $[\mathrm{diag}(1, 1, p, p)]$ and eventually to $[\mathrm{diag}(1, p, p, p)]$, which is connected back to $[I]$. We now have a cycle of length 4, and in the building it will be completed to a *tetrahedron*, so that we also add the edge $[I] \to [\mathrm{diag}(1, 1, p, p)]$, and then the face $\{[I], [\mathrm{diag}(1, 1, 1, p)], [\mathrm{diag}(1, p, p, p)]\}$, the face $\{[I], [\mathrm{diag}(1, 1, 1, p)], [\mathrm{diag}(1, 1, p, p)]\}$, and so on. We simply complete the entire cycle to a 4-simplex. This way, we loose the directedness.

Definition 18 (Bruhat-Tits Building of $\mathrm{PGL}_d(\mathbb{Q}_p)$)**.** The Bruhat-Tits building of $G = \mathrm{PGL}_d(\mathbb{Q}_p)$ is a simplicial complex with vertex set G/K, where $K = \mathrm{PGL}_d(\mathbb{Z}_p)$. Connect a coset gK with a directed edge to $g\,\mathrm{diag}(1, \dots, 1, p)K$. Now complete every d-cycle to a $(d-1)$-simplex. The building is written $\mathcal{X}_d$ or $\mathcal{B}(\mathrm{PGL}_d(\mathbb{Q}_p))$.

Notice that there are many g' with $gK = g'K$, so that the graph is not 1-out-regular: we connect each gK to $g'\,\mathrm{diag}(1, \dots, 1, p)K$ with $g'K = gK$, and some of these may be different in G/K. For example, $[\mathrm{diag}(1, 1, 1, p)]$ is also represented by $\begin{bmatrix} 1 & & & \\ & & & 1 \\ & & 1 & \\ & p & & \end{bmatrix}$, which we connect to $[\mathrm{diag}(1, p, 1, p)]$ (which is different from $[\mathrm{diag}(1, 1, 1, p^2)]$, to which $[\mathrm{diag}(1, 1, 1, p)]$ is also connected).

Definition 19. There are alternative definitions, in the language of lattices:

1. Construct an edge between L and L' if $pL' < L < L'$ or $pL < L' < L$, and then "clique-ify" - take the clique complex; for any j-clique in the graph, declare its vertices as a $(j-1)$-simplex.

2. The collection of lattices $\{L_1, \ldots, L_j\}$ is a cell if and only if, possibly after reordering,

$$pL_1 < L_j < \cdots < L_2 < L_1.$$

Try convincing yourself these indeed work in the example above of a cell in the building of PGL_4, and that these are indeed equivalent (this is not very easy).

A corollary to these definitions is that the dimension of a maximal cell in the building is at most $d-1$, since $L_1/pL_1 \cong \mathbb{F}_p^d$ doesn't have longer chains of subgroups. It is *exactly* $d-1$, because $\{\mathbb{Z}_p^d, p\,\mathbb{Z}_p \times \mathbb{Z}_p^{d-1}, \ldots, \mathbb{Z}_p \times (p\,\mathbb{Z}_p)^{d-1}\}$ is a cell, called the *Fundamental chamber*. A *chamber* is a cell of dimension $d-1$.

Definition 20 (Edge-Coloring of the Building)**.** Color a directed edge $L \to L'$ in the building with the color $\mathrm{val}_p[L' : L]$ if $pL' < L < L'$ and with the color $d - \mathrm{val}_p[L' : L]$ if $pL' < L < L'$. This is a coloring map to $(\mathbb{Z}/d\,\mathbb{Z})^\times$. Equivalently, we can color $gK \to hK$ with $\mathrm{val}_p \det g^{-1}h \pmod d$. Notice that even though g, h are defined up to scaling, if we scale one of them by, say, α, the determinant is scaled by α^d, so that the valuation varies by some integer multiple of d. But the coloring is in $(\mathbb{Z}/d\,\mathbb{Z})^\times$, so this is well-defined.

The coloring just measures how many factors of p we added in the determinant, e.g. the edge from $[\mathrm{diag}(1, 1, 1, p)]$ to $[\mathrm{diag}(p, p, 1, p)]$ will be colored 2. It is easy to see the color of $v \to w$ is the additive inverse of the color of $w \to v$.

The edges of the form $gK \to g\,\mathrm{diag}(1, \ldots, 1, p)K$ are precisely the edges of color 1, (sometimes called 1-*edges*). As in the definition, these give rise to the entire building.

How does the 'area around a vertex' look like? We want to describe all cells containing $v_0 = \mathbb{Z}_p^d$ (we can then move to gv_0 for any $g \in G$). Indeed, $\{v_0, v_1, \ldots, v_j\}$ is a cell if and only if the corresponding lattices $L_0, \ldots, L_j$ satisfy that, up to reordering, $pL_0 < L_j < \cdots < L_1 < L_0$. We want to use the correspondence theorem, but how do we deal with this reordering? Well, $\{L_0, \ldots, L_j\}$ is a cell if and only if there exists some $\pi \in S_{j+1}$ so that $pL_{\pi(0)} < L_{\pi(j)} < \cdots < L_{\pi(0)}$. But this chain can be continued in both directions:

$$\cdots < pL_{\pi(1)} < pL_{\pi(0)} < L_{\pi(j)} < \cdots < L_{\pi(0)} < p^{-1}L_{\pi(j)} < p^{-1}L_{\pi(j-1)} < \cdots$$

But now $L_0 = L_{\pi(\pi^{-1}(0))}$, so it is somewhere in the middle of that chain. Taking the elements to its left, we find that each cell containing $v_0 = \mathbb{Z}_p^d$ *does* correspond to a chain between pL_0 and L_0 (i.e. $p\,\mathbb{Z}_p^d$ and $\mathbb{Z}_p^d$). But these correspond to flags in $\mathbb{Z}_p^d/p\,\mathbb{Z}_p^d \cong \mathbb{F}_p^d$ (a *flag in* $\mathbb{F}_p^d$ is a sequence of subspaces $0 < V_1 < \cdots < V_j < \mathbb{F}_p^d$).

It is evident that the neighbors of $\mathbb{Z}_p^d$ which form an edge of color 1 are those which have 1's on the diagonal, except for one place in which it has p and on its left there are elements in $\mathbb{Z}/p\,\mathbb{Z}$. The neighbors which form an edge of color 2 have two p's on the diagonal and elements on their left (which satisfy some additional conditions), and so on. We now see that 1-edges correspond to $(d-1)$-dimensional subspaces of $\mathbb{F}_p^d$, 2-edges correspond to $(d-2)$-dimensional subspaces of $\mathbb{F}_p^d$, and so on, and that such a collection forms a triangle if and only if they form a flag. For example, if $\mathbb{Z}_p^d$ is connected via a 1-edge to V and via a 2-edge to W, $\{\mathbb{Z}_p^d, V, W\}$ forms a triangle if and only if $W < V$ (here we abuse notation and assume that a vertex is a subspace of $\mathbb{F}_p^d$). More concretely:

Example 13. The vertices $[I], [\mathrm{diag}(1, 1, p)], [\mathrm{diag}(p, 1, p)]$ form a triangle in the building of PGL_3, but the vertices $[I], [\mathrm{diag}(1, 1, p)], [\mathrm{diag}(p, p, 1)]$ do not. The latter two are, however, connected to the first.

To sum up: *Neighbors of* $\mathbb{Z}_p^d$ *are in correspondence with non-trivial subspaces of* $\mathbb{F}_p^d$*, and cells containing* $\mathbb{Z}_p^d$ *are in correspondence with flags in* $\mathbb{F}_p^d$*.*

The number of j-dimensional subspaces of $\mathbb{F}_p^d$ is written $\binom{d}{j}_p$, and is sometimes called a *Gaussian binomial coefficient*. It can be shown $\binom{d}{1}_p = \frac{p^d-1}{p-1}$, $\binom{d}{2}_p = \frac{(p^d-1)(p^{d-1}-1)}{(p^2-1)(p-1)}$, and so on. The degree of any vertex in the building is thus $\sum_{j=1}^{d-1}\binom{d}{j}_p$.

How many chambers (maximal cells) are there containing v_0? These are in correspondence with maximal flags (JH sequences) in $\mathbb{F}_p^d$. It is easy to count and see that this number is equal to:

$$\frac{p^d-1}{p-1}\cdot\frac{p^{d-1}-1}{p-1}\cdots\frac{p-1}{p-1}=p^{\frac{d(d-1)}{2}}(1+o(1/p))$$

Claim. *$K = \mathrm{PGL}_d(\mathbb{Z}_p) = \mathrm{Stab}_G(v_0)$ acts transitively on chambers containing v_0. G acts transitively on chambers, and even on pointed chambers (i.e. on the collection (σ, v) with σ a chamber and $v \in \sigma$ a vertex).*

Proof. K acts on the neighbors of v_0 by $K \twoheadrightarrow \mathrm{PGL}_d(\mathbb{F}_p)$ acting on subspaces of $\mathbb{F}_p^d$ (as we saw for $d = 2$). The map here is the modulo p map. But $\mathrm{PGL}_d(\mathbb{F}_p)$ acts transitively on *maximal* flags in $\mathbb{F}_p^d$, which correspond to chambers. Indeed, for any flag $V_0 < \cdots < V_d$ there exists a basis $b_1, \ldots, b_d$ with $V_j = \mathrm{Span}\{b_1, \ldots, b_j\}$; the claim is now clear. The claim on the action of G is now clear. □

Claim. *Let σ_0 be the fundamental chamber. The pointwise stabilizer of σ_0 under the action of G is the Iwahori subgroup B, which is the preimage of the subgroup of $\mathrm{GL}_d(\mathbb{F}_p)$ of upper-triangular matrices under the modulo p map.*

Proof. One way to see this is to show:

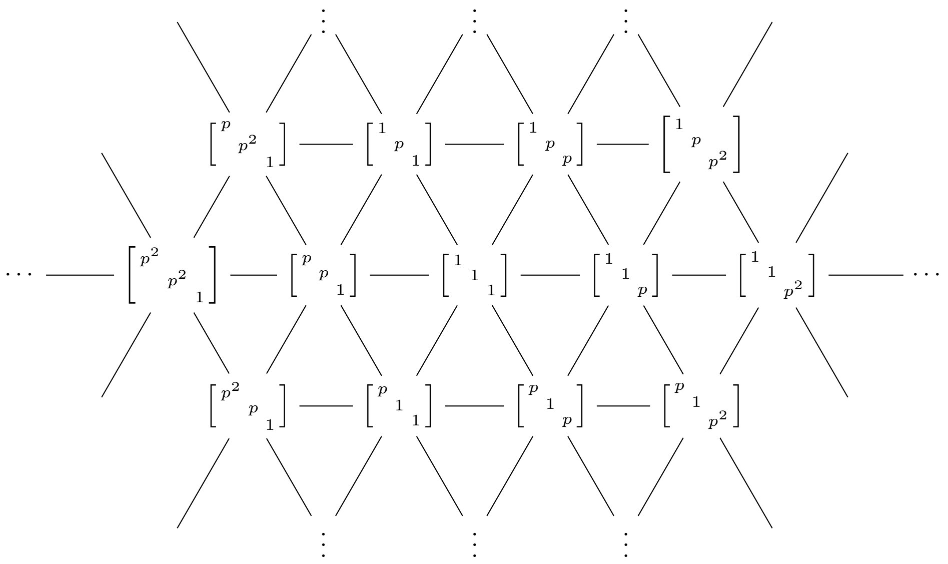
$$B=\bigcap_{j=1}^{d-1}\mathrm{diag}(1,\ldots,1,\underbrace{p,\ldots,p}_{\times j})K\,\mathrm{diag}(1,\ldots,1,\underbrace{p,\ldots,p}_{\times j})^{-1}$$

Another way is to note σ_0 corresponds to the standard maximal flag in $\mathbb{F}_p^d$. The $\mathrm{GL}_d(\mathbb{F}_p)$-stabilizer of this flag in $\mathbb{F}_p^d$ is the subgroup of upper-triangular matrices. Thus $\mathrm{Stab}_G(\sigma_0) = \mathrm{Stab}_K(\sigma_0)$ is the desired preimage through $K \to \mathrm{GL}_d(\mathbb{F}_p)$. □

The action of G on the chambers is transitive and the pointwise stabilizer of a chamber is B. Thus G/B is in correspondence with pointed chambers. Check that B is also the G-stabilizer of a pointed chamber (σ_0, v_0) (here, the stabilizer is not pointwise on σ_0).

Recall that for $d = 2$ we had B as a stabilizer of a pointed edge, and $B\backslash\mathcal{X}_2^0 = B\backslash G/K$ was in a one-to-one correspondence with $A = \{\mathrm{diag}(p^{m_i}) : \min m_i = 0\}$. This follows, from example, from the decomposition $G = \bigsqcup_{a\in A} BaK$.

Let $\mathcal{A}$ be the subcomplex spanned by Av_0, i.e. the subcomplex consisting of diagonal matrices, rescaled so that the minimal power is 0. The case $d = 3$ is partially drawn below.


$\begin{bmatrix}p&&\\&p^2&\\&&1\end{bmatrix}$
$\begin{bmatrix}1&&\\&p&\\&&1\end{bmatrix}$
$\begin{bmatrix}1&&\\&p&\\&&p\end{bmatrix}$
$\begin{bmatrix}1&&\\&p&\\&&p^2\end{bmatrix}$
$\begin{bmatrix}p^2&&\\&p^2&\\&&1\end{bmatrix}$
$\begin{bmatrix}p&&\\&p&\\&&1\end{bmatrix}$
$\begin{bmatrix}1&&\\&1&\\&&1\end{bmatrix}$
$\begin{bmatrix}1&&\\&1&\\&&p\end{bmatrix}$
$\begin{bmatrix}1&&\\&1&\\&&p^2\end{bmatrix}$
$\begin{bmatrix}p^2&&\\&p&\\&&1\end{bmatrix}$
$\begin{bmatrix}p&&\\&1&\\&&1\end{bmatrix}$
$\begin{bmatrix}p&&\\&1&\\&&p\end{bmatrix}$
$\begin{bmatrix}p&&\\&1&\\&&p^2\end{bmatrix}$

We call $\mathcal{A}$ the *fundamental apartment*, and for $d = 3$ it is a triangulation of the plane $\mathbb{R}^2$. This is one of several possible triangulations of the plane with congruent triangles, and theoretically we could have picked any other one. However, it can be shown this specific choice makes G act by Euclidean isometries (translations and reflections of the plane). This has to do with the structure of the corresponding Weyl group as a Coxeter group.

In general, $\mathcal{A} \subseteq \mathcal{X}_d$ is a triangulation of $\mathbb{R}^{d-1}$ by $(d-1)$-simplices. In the apartment, every $(d-2)$-cell is a susbet of 2 $(d-1)$-cells.

Claim. $\mathcal{A} \cong B \backslash \mathcal{X}_d$.

Proof. For vertices, $B\backslash\mathcal{X}_d^0 \cong B\backslash G/K \leftrightarrow A \leftrightarrow \mathcal{A}^0$. For chambers, $B\backslash\mathcal{X}_d^{d-1} \cong B\backslash G/B \leftrightarrow W$. Indeed, if σ is a chamber and $\sigma = g\sigma_0$, we can write $g = bwb'$ so $\sigma = bwb'\sigma_0 = bw\sigma_0$, so $b^{-1}\sigma = w\sigma_0$ for some $w \in W$. Now $b^{-1}\sigma = w\sigma_0 \in \mathcal{A}$. In words, *we can use B to move from any chamber to a chamber in the fundamental apartment.* As an exercise, show that $W = N_G(A) = \mathrm{Stab}(\mathcal{A}^0)$. The first equality is group-theoretic, and the latter is set-theoretic. □

This shows that the apartment is a flattening of the building, in some sense.

We now give a few observations.

1. W acts simply transitively on pointed chambers in $\mathcal{A}$. This uses the fact $W = S_d \ltimes A$. Take (σ_0, v_0) and (σ, v). We then show there exists a unique $a \in A$ with $av = v_0$, and a unique $\pi \in S_d$ with $\pi a\sigma = \sigma_0$. The 'simply' part follows from $\mathrm{Stab}_W((\sigma_0, v_0)) = \mathrm{Stab}_G((\sigma_0, v_0)) \cap W = B \cap W = 1$.
2. The following matrix acts simply transitively on $\{(\sigma_0, v) : v \in \sigma_0\}$, and generates the cyclic group $\mathbb{Z}/d\mathbb{Z}$:
$$\begin{pmatrix} 0 & 1 & & & & \\ & 0 & 1 & & & \\ & & 0 & 1 & & \\ & & & \ddots & \ddots & \\ & & & & \ddots & 1 \\ p & & & & & 0 \end{pmatrix}$$
3. S_d acts by permuting the entries, $\pi.aK = \pi a\pi^{-1}K$.
4. S_d acts simply transitively on $\{(\sigma, v_0) : \sigma \in \mathcal{A}\}$. This is because neighbors of v_0 are in correspondence with subspaces of $\mathbb{F}_p^d$, chambers containing v_0 are in correspondence with maximal flags in $\mathbb{F}_p^d$ and neighbors of v_0 in $\mathcal{A}$ correspond to subspaces generated by subsets of the standard basis. This means chambers containing v_0 in $\mathcal{A}$ are in correspondence with maximal flags generated using the standard basis, and these correspond to permutations.

We saw that $\mathrm{PGL}_2(\mathbb{Q}_p)$ acts transitively on the set of infinite half-lines through the tree.

Definition 21 (Apartment)**.** An *apartment* in $\mathcal{X}_d$ is a G-translation of $\mathcal{A}$, i.e. the subcomplex $g\mathcal{A}$ generated by gAv_0 for some $g \in G$.

Vertices of $\mathcal{A}$ correspond to lattices of the form $\mathrm{Span}_{\mathbb{Z}_p}(\{p^{m_i}e_i\})$. Vertices of $g\mathcal{A}$ correspond to lattices of the form $\mathrm{Span}_{\mathbb{Z}_p}(\{p^{m_i}ge_i\})$, which corresponds to $\mathrm{Span}_{\mathbb{Z}_p}(\{p^{m_i}v_i\})$ for $\{v_i\}$ a basis of $\mathbb{Q}_p^d$.

From now on we denote the fundamental apartment by $\mathcal{A}_0$ and any apartment by $\mathcal{A}$.

Definition 22 (Simplicial Affine Building)**.** A *d-dimensional simplicial affine building* is a simplicial complex $\mathcal{B}$ equipped with a set of subcomplexes called *apartments*, such that:

1. Each apartment is a simplicial tesselation of $\mathbb{R}^d$, i.e. a triangulation attained by starting with one d-simplex and reflecting on its faces,
2. For any $\sigma, \sigma' \in \mathcal{B}$ there exists an apartment $\mathcal{A}$ with $\sigma, \sigma' \in \mathcal{A}$,

3. If $\sigma, \sigma' \in \mathcal{A}, \mathcal{A}'$ then there exists an automorphism φ of $\mathcal{B}$ such that $\varphi(\mathcal{A}) = \mathcal{A}'$ and $\varphi(\sigma) = \sigma, \varphi(\sigma') = \sigma'$.

We can erase the word 'simplicial' in the definition (and perhaps replace it with 'polyhedral'), and we get a more general definition of a building. We can also replace $\mathbb{R}^d$ with S^d or $\mathbb{H}^d$, and attain a definition for a *spherical* or *hyperbolic* building.

Theorem 14. *The complex $\mathcal{X}_d$ is a building with system of apartments $\{g\mathcal{A}_0 : g \in G\}$.*

Proof. Let $\sigma, \sigma' \in \mathcal{X}_d^{d-1}$. We want to find $g \in G$ with $\sigma, \sigma' \in g\mathcal{A}_0$. We can assume $\sigma = \sigma_0$. Write $\sigma' = g'\sigma_0$ with $g' \in G$. As usual, write $g' = bwb'$, so that $\sigma' = bw\sigma_0$. Since $w\sigma_0$ is in $\mathcal{A}_0$, the apartment $b\mathcal{A}_0$ contains both σ_0 and σ'. This also works for $G = \mathrm{PGL}_d(\mathbb{Z}[p^{-1}])$, since the decomposition $G = BWB$ still holds.

Now assume $\sigma_0, \sigma' \in \mathcal{A}', \mathcal{A}''$. We want to find a $g \in G$ fixing σ_0, σ' with $g\mathcal{A}' = \mathcal{A}''$. Write $\sigma' = bw\sigma_0$. Now, $b\mathcal{A}_0$ contains σ_0 and σ'. Assume $\sigma_0, \sigma' \in g\mathcal{A}_0$, some other apartment. In particular, $\sigma_0 = gw'\sigma_0$ for some $w \in W$, which means $gw' \in B$. Since $g\mathcal{A}_0 = gw'\mathcal{A}_0$ we can assume $g = b' \in B$ to begin with. This means $\sigma_0, \sigma' = bw\sigma_0 \in b\mathcal{A}_0, b'\mathcal{A}_0$. Because $bw\sigma_0 \in b'\mathcal{A}_0$, there exists some w'' with $bw\sigma_0 = b'w''\sigma_0$. This is equivalent to saying $bwB = b'w''B$, but uniqueness tells us $w = w''$, so that $b'b^{-1} : b\mathcal{A}_0 \to b'\mathcal{A}_0 = g\mathcal{A}_0$ and it also fixes σ_0 and σ since $b'b^{-1}bw\sigma_0 = b'w''\sigma_0 = bw\sigma_0$. □

Try to decode this proof and gain an intuition for it. Another proof is given in the course's website. Consider the fundamental apartment of the tree; it has two sides: the "left" side consisting of diagonal matrices of the form $\mathrm{diag}(p^n, 1)$ for $n \geq 1$, and the "right" side consisting of diagonal matrices of the form $\mathrm{diag}(1, p^n)$ for $n \geq 1$. The fibers of the "left" side under the projection are nice: for $\mathrm{diag}(p, 1)$ its $\left(\begin{smallmatrix} p & x \\ & 1 \end{smallmatrix}\right)$ for $x \in \mathbb{Z}/p$, for $\mathrm{diag}(p^2, 1)$ it's the same but with p^2 and $x \in \mathbb{Z}/p^2$ and so on.

The analog of this for the two-dimensional apartment in PGL_3 is the sector consisting of diagonal matrices with decreasing powers; that is to say, if $\pi : \mathcal{B} \to \mathcal{A}_0$ is the projection under the action of B, then for $a = \mathrm{diag}(p^{m_1}, \ldots, p^{m_d})$ with $m_1 \geq \cdots \geq m_d = 0$ we have $\pi^{-1}(a)$ as the matrix with p^{m_i} along the diagonal and b_{ij} above them with $p^{m_j} \mid b_{ij} \in \mathbb{Z}/p^{m_i}$.

6 Buildings for Other Groups

6.1 Buildings for Classical Groups

Consider the orthogonal group $O_n(\mathbb{Q}_p) = \{g \in \mathrm{GL}_n(\mathbb{Q}_p) : gg^t = I\}$. The key observation here is that this is the collection of the fixed points of the involution $\# : G \to G$ with $g^\# = (g^t)^{-1}$, where $G = \mathrm{GL}_n$ (this is the unique outer automorphism of G up to conjugation). In general, let $H \in \mathrm{GL}_n(\mathbb{Q}_p)$ be symmetric, and define $O(H) = O_n(\mathbb{Q}_p, H) = \{g \in G : gHg^t = H\}$. The corresponding involution is now $g^\# = H(g^t)^{-1}H^{-1}$. We write $O(H) = G^\#$, the subgroup of fixed elements under the involution. We want to define a corresponding involution on $\mathcal{B}(G)$. Begin with vertices. Write $v = gv_0$. Can we try to define $v^\# = g^\# v_0$? This turns out not to work; this is not well-defined. For us to define $v^\#$ appropriately, first note that $(gK)^\# = g^\# K^\#$. This means that we have a map $\# : G/K \to G/K^\#$. Now, G/K corresponds to $\mathcal{B}^0$ (under $gK \mapsto gv_0$), but so does $G/K^\#$! Indeed, notice that $K^\# = HKH^{-1}$, so that $K^\# = \mathrm{Stab}_G(Hv_0)$. This means the map $gK^\# \mapsto gHv_0$ gives a correspondence with $\mathcal{B}^0$. Composing these maps together, we get the involution $\mathcal{B}_0 \to \mathcal{B}_0$ given by $gv_0 \mapsto g^\# Hv_0$. This is now well-defined. In the same way we have $O(H) = G^\#$, we want to have $\mathcal{B}(O(H)) = \mathcal{B}^\#$. Except for a few special cases, this is true. A more accurate way of writing this would be $\mathcal{B}(\mathrm{PO}(H)) = \mathcal{B}(\mathrm{PGL}_n)^\#$.

We now deviate and note that if H is anti-symmetric, the group $G^\# = \mathrm{Sp}(H)$ is called a *symplectic group*. If $E/\mathbb{Q}_p$ is a quadratic Galois extension and $H \in \mathrm{GL}_n(E)$ is Hermitian (i.e. $H^*_{ij} = \tau(H_{ji})$ where τ is non-trivial element in the Galois group), we obtain the unitary group $U(H)$ (which fixes $g^\# = H(g^*)^{-1}H^{-1}$). These allow us to define the buildings of Sp and U, where in the last case $\mathcal{B}(U(H)) = \mathcal{B}(\mathrm{PGL}_n(E))^\#$ (and not $\mathrm{PGL}_n(\mathbb{Q}_p)$).

Back to the orthogonal case.

Claim. *The involution $\#$ acts simplicially on $\mathcal{B} = \mathcal{B}(\mathrm{PGL})$, i.e. takes simplices to simplices.*

Proof. It is enough to show $\#$ takes edges to edges, since $\mathcal{B}$ is a clique complex. Thus we want to show that if $gv_0 \sim hv_0$ then $g^\# Hv_0 \sim h^\# Hv_0$. Note that $(gv_0)^\# = g^\# Hv_0 = H(g^t)^{-1}v_0$, so that the last statement is equivalent to $H(g^t)^{-1}v_0 \sim H(h^t)^{-1}v_0$, which is in turn equivalent to $(g^t)^{-1}v_0 \sim (h^t)^{-1}v_0$ or $v_0 \sim ((g^{-1}h)^t)^{-1}v_0$. Write $s = g^{-1}h$. Our assumption can now be restated as $sv_0 \sim v_0$. This implies $KsK = K\,\mathrm{diag}(1, 1, \ldots, 1, p, \ldots, p)K$; this follows from the $G = KA^+K$ decomposition: if $s = kak'$ then $KsK = Kkak'K = KaK$, but also $av_0 \sim v_0$ because $kak'v_0 \sim v_0$. Denote $s_j = \mathrm{diag}(1, \ldots, 1, p, \ldots, p)$ with the 1 taken $\times j$ times. We want $(s^t)^{-1}v_0 \sim v_0$. But $K(s^t)^{-1}K = ((KsK)^t)^{-1} = ((Ks_jK)^t)^{-1}$, and $K(s_j^t)^{-1}K = Ks_{d-j}K$ which implies $(s^t)^{-1}v_0 \sim v_0$. We conclude $(gv_0)^\# \sim (hv_0)^\#$. □

The proof above shows that $\#$ flips colors!

Claim. *We have $(gv)^\# = g^\# v^\#$. In particular, $O(H)$ is given by the action of $G^\#$ on $\mathcal{B}^\#$.*

Proof. If $v = hv_0$ we get $(ghv_0)^\# = (gh)^\# Hv_0 = g^\#(h^\# Hv_0) = g^\#(hv_0)^\#$. The corollary now follows because if $g^\# = g$ and $v^\# = v$ then $(gv)^\# = gv$. □

We want an H which gives nice results which are comfortable to work with. In particular, we'd like $v_0^\# = v_0$, which is equivalent to $H \in K$. We also want $\#$ to take the fundamental apartment to itself (or equivalently $A^\# = A$). This is equivalent to H being monomial, once we chose $H \in K$. The last thing we require is that $B^\# = B$. This turns out to be equivalent to H having non-zero elements only on the *secondary* diagonal, which have to be invertible elements in $\mathbb{Z}_p$. We arrive at the canonical choice of H having 1's along the secondary diagonal and 0's elsewhere.

Now, using the BAK decomposition, we arrive at the projection $\mathcal{B}^0 \to \mathcal{A}_0^0$. Since $\#$ fixes B, A, K, we get the following commutative diagram:

$$\begin{tikzcd}
\mathcal{B}^0 \arrow[r, "\#"] \arrow[d, "\pi"'] & \mathcal{B}^0 \arrow[d, "\pi"] \\
\mathcal{A}_0^0 \arrow[r, "\#"'] & \mathcal{A}_0^0
\end{tikzcd}$$

In terms of actual elements, start with some vertex $gv_0 = bav_0$, and then using uniqueness of the A in the BAK decomposition:

$$\begin{tikzcd}
bav_0 \arrow[r, "\#"] \arrow[d, "\pi"'] & b^\# a^\# v_0 \arrow[d, "\pi"] \\
av_0 \arrow[r, "\#"'] & a^\# v_0
\end{tikzcd}$$

We arrive at the following corollary:

Claim. *If $v \in \mathcal{B}^\#$ then $\pi(v) \in \mathcal{A}_0^\#$*

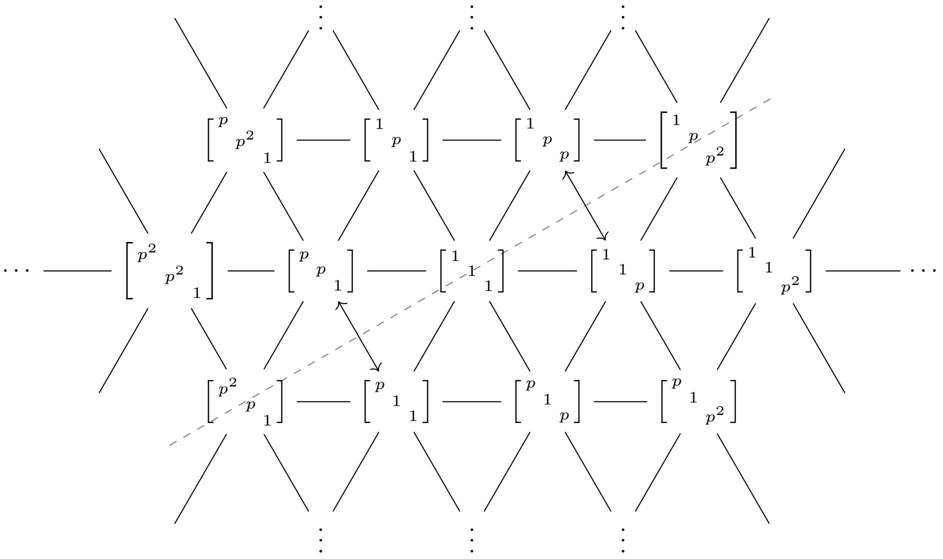
We emphasize that $G^\#, \mathcal{B}^\#, \mathcal{A}_0^\#$ mean the collection of fixed points of the corresponding object under $\#$, and any other $^\#$ on an object means the collection of the $^\#$ of all elements in the collection.

Proof. If $v = v^\#$ then $\pi(v)^\# = \pi(v^\#) = \pi(v)$. □

This means $\mathcal{B}^\# \subseteq \pi^{-1}(\mathcal{A}_0^\#)$.

6.2 The case $n = 3$

Let us find the building of $O(3)$ and its fundamental apartment. Define $J = \begin{pmatrix} & & 1 \\ & 1 & \\ 1 & & \end{pmatrix}$. Now notice that if $a = \mathrm{diag}(p^m, p^n, p^\ell)$ with $\min(m, n, \ell) = 0$, then $a^\# = \mathrm{diag}(p^{-\ell}, p^{-n}, p^{-m})$. Now we ask when $a = a^\#$ *in the group* PGL, i.e. up to a constant. Looking at the middle element we see we must scale by $2n$, so that $a = a^\#$ if and only if $m + \ell = 2n$. This means that $a = \mathrm{diag}(p^{2n}, p^n, 1)$ or $a = \mathrm{diag}(1, p^n, p^{2n})$. The involution is thus represented by a reflection along the dashed line in the following drawing.


$\begin{bmatrix}p&&\\&p^2&\\&&1\end{bmatrix}$
$\begin{bmatrix}1&&\\&p&\\&&1\end{bmatrix}$
$\begin{bmatrix}1&&\\&p&\\&&p\end{bmatrix}$
$\begin{bmatrix}1&&\\&p&\\&&p^2\end{bmatrix}$
$\cdots$
$\begin{bmatrix}p^2&&\\&p^2&\\&&1\end{bmatrix}$
$\begin{bmatrix}p&&\\&p&\\&&1\end{bmatrix}$
$\begin{bmatrix}1&&\\&1&\\&&1\end{bmatrix}$
$\begin{bmatrix}1&&\\&1&\\&&p\end{bmatrix}$
$\begin{bmatrix}1&&\\&1&\\&&p^2\end{bmatrix}$
$\cdots$
$\begin{bmatrix}p^2&&\\&p&\\&&1\end{bmatrix}$
$\begin{bmatrix}p&&\\&1&\\&&1\end{bmatrix}$
$\begin{bmatrix}p&&\\&1&\\&&p\end{bmatrix}$
$\begin{bmatrix}p&&\\&1&\\&&p^2\end{bmatrix}$

We now compute that:

$$\pi^{-1}\begin{pmatrix}p^{2n}&&\\&p^n&\\&&1\end{pmatrix}=\left\{\begin{pmatrix}p^{2n}&ap^n&b\\&p^n&c\\&&1\end{pmatrix}:a,c\in\mathbb{Z}/p^n,b\in\mathbb{Z}/p^{2n}\right\}$$

Denote this matrix by $g_{n,a,b,c}$. For which a,b,c do we get $g^{\#}_{n,a,b,c}K=g_{n,a,b,c}K$, i.e. they represent the same vertex? A simple computation gives, up to scaling:

$$g^{\#}_{n,a,b,c}=\begin{pmatrix}p^{2n}&-cp^n&ac-b\\&p^n&-a\\&&1\end{pmatrix}$$

We want to have $g^{\#}_{n,a,b,c}K=g_{n,a,b,c}K$ (equivalently $g^{\#}_{n,a,b,c}v_0=g_{n,a,b,c}v_0$), and this implies $c=-a$ (recall these are elements of $\mathbb{Z}/p^n$), and $ac-b=b$ (in $\mathbb{Z}/p^{2n}$). Thus $2b\equiv -a^2\pmod{p^{2n}}$. This condition, together with $a=-c$, are sufficient and necessary for us to have $g^{\#}_{n,a,b,c}K=g_{n,a,b,c}K$. We now have to split to cases.

Assume $p\neq 2$. Then $b\equiv -\frac{a^2}{2}\pmod{p^{2n}}$. We obtain:

$$\mathcal{B}^{\#}=\left\{\begin{pmatrix}p^{2n}&ap^n&-\frac{a^2}{2}\\&p^n&-a\\&&1\end{pmatrix}:a\in\mathbb{Z}/p^n,n\in\mathbb{N}\right\}\cup\left\{\begin{pmatrix}1&&\\&p^n&\\&&p^{2n}\end{pmatrix}\right\}$$

These give us the matrices which lie "above" a given orthogonal diagonal matrix in the "principal sector" (defined as the lower-left sixth-sector) in the building. In any case, with some more handwaving, we can see this is in fact a $(p+1)$-regular tree. In fact, for $p\neq 2$, $\mathrm{SO}(\mathbb{Q}_p,J)\cong\mathrm{SL}_2(\mathbb{Q}_p)$ where J is our form. In particular, the building is as expected.

Now let's take $p=2$. The condition becomes $2b\equiv -a^2\pmod{2^{2n}}$, so a has to be even and $b\equiv -\frac{a^2}{2}$ (mod 2^{2n-1}) (where the division happens in the integers). This means that once we choose some even a, our choice of b is not unique: we can take such b and also $b+2^{2n-1}$. We have less freedom in our choice of a and more freedom in our choice of b. For example, "above" $\mathrm{diag}(4,2,1)$ in the fundamental apartment, we have $\begin{pmatrix}4&&2\\&2&\\&&1\end{pmatrix}$. This matrix is connected to both $\mathrm{diag}(2,2,1)$ and $\mathrm{diag}(2,1,1)$, which are both connected also to $\mathrm{diag}(4,2,1)$. Thus we have "two triangles above each other". v_0 is also a vertex of the triangle with two other vertices $\begin{pmatrix}2&&1\\&2&\\&&1\end{pmatrix}$, $\begin{pmatrix}2&&1\\&1&\\&&1\end{pmatrix}$. These matrices are flipped under the involution. This goes one: each orthogonal matrix lies on two triangles, one of which is 'wrong' and 'continues nowhere', and the other one is connected to two other triangles, closing the rhombus. The construction thus begins with a vertex, connects it to an edge which goes nowhere and an edge whose endpoint splits again to two edges, and so on. In some definitions, this is what we call the building of $O(\mathbb{Q}_2)$, but in some other constructions/definitions of the building, we ignore the 'wrong directions', and then we are left with a 3-regular tree. The 'wrong directions' are called *barbs*.

We took a nice H for our use, but what happens if we choose a different one? Taking P^tHP gives the same result for any P. In $\mathbb{Q}_3$, define $P = \frac{1}{2}\begin{pmatrix} 1 & \sqrt{-2} & 1 \\ 1 & -\sqrt{-2} & 1 \\ \sqrt{-2} & 0 & -\sqrt{-2} \end{pmatrix}$, with the square roots arising from Hensel's lemma. It can be checked that $P^tP = \begin{pmatrix} & & 1 \\ & -1 & \\ 1 & & \end{pmatrix}$. This means that $O_3(\mathbb{Q}_3, I) \cong O_3\left(\mathbb{Q}_3, \begin{pmatrix} & & 1 \\ & -1 & \\ 1 & & \end{pmatrix}\right)$. The latter is of the form we like (recall the conditions we imposed on H), so analysis on it would be nice.

For $U_3(\mathbb{Q}_p, I)$ we get $O_3\left(\mathbb{Q}_3, \begin{pmatrix} & & 1 \\ & \pm 1 & \\ 1 & & \end{pmatrix}\right)$ if $p \neq 2$ and some compact group if $p = 2$. The building of $U_3(\mathbb{Q}_2)$ would be a single point, but if we consider it the way we did with involutions, we actually get a point with barbs: a star with 4 vertices.

A moment on pedagogy: most literature does not describe the buildings this way (they usually talk about BN-pairs, root structure theory etc.). There are only a few papers regarding this approach, but it is very nice and gives good intuition.

7 Finite Quotients - Crash Course

We know that when we quotient the plane $\mathbb{R}^2$ by the discrete subgroup $\mathbb{Z}^2$ we get a torus. In the hyperbolic case, if we quotient $\mathbb{H}^2 = \mathrm{PGL}_2(\mathbb{R})/O(2)$ by $\mathrm{PGL}_2(\mathbb{Z})$ (which is a subgroup of the automorphism group of $\mathbb{H}^2$), we obtain the modular surface, which is the fundamental domain for the action, $Y_1 = \{-1/2 \leq \operatorname{Re} z \leq 1/2\} \setminus \{|z| \leq 1\}$, glued at specific points. If we define $\Gamma(N) = \{\gamma \in \mathrm{PGL}_2(\mathbb{Z}) : \gamma \equiv I \mod N\}$ we obtain a normal subgroup of $\mathrm{PGL}_2(\mathbb{Z})$, and the quotients Y_N of the hyperbolic plane by these give us Riemann surfaces. We now consider the p-adic analogue.

Recall $\mathcal{B}_{2,p} = T_{p+1} = \mathrm{PGL}_2(\mathbb{Q}_p)/\mathrm{PGL}_2(\mathbb{Z}_p)$. Since $\mathbb{Z}$ is not discrete in $\mathbb{Q}_p$, it is not a good choice for our quotient. Also, $\mathrm{PGL}_2(\mathbb{Z})$ fixes v_0, and the quotient $\mathrm{PGL}_2(\mathbb{Z})\backslash T_{p+1}$ will be an infinite line, so it also doesn't behave how we want. We want to switch to $\mathrm{PGL}_2(\mathbb{Z}[p^{-1}])$, which acts interestingly (transitively etc.), but this subgroup is still not discrete. It turns out $\mathbb{Z}[p^{-1}]$ is not discrete in $\mathbb{Q}_p$ nor in $\mathbb{R}$, but it is discrete in the product $\mathbb{R} \times \mathbb{Q}_p$. Indeed, if $a_n p^{m_n} \to_{\mathbb{R}} 0$ with $p \nmid a_n \in \mathbb{Z}$, then $m_n \to -\infty$, which implies $a_n p^{m_n} \not\to_{\mathbb{Q}_p} 0$. Let $G = \mathrm{PGL}_2$. We get that $G(\mathbb{Z}[p^{-1}]) \leq G(\mathbb{R} \times \mathbb{Q}_p) = G(\mathbb{R}) \times G(\mathbb{Q}_p)$ discretely. But this latter group acts on $\mathbb{H}^2 \times T_{p+1}$. Thus, for $p \nmid N$, we can define $\Gamma(N) = \{\gamma \in G(\mathbb{Z}[p^{-1}]) : \Gamma \equiv I \ (N)\}$ and then study $\Gamma(N)\backslash\mathbb{H}^2 \times T_{p+1}$. The object $\mathbb{H}^2 \times T_{p+1}$ can be thought of as the tree with a copy of the hyperbolic point at every vertex, and the quotient can be thought of as a finite graph with a Riemann surface at every point. What if we don't want to study Riemann surfaces and the like? After all, we only added the hyperbolic plane to get $\mathbb{Z}[p^{-1}]$ as a discrete subgroup. The idea is to recall T_{p+1} is also the building of $O_3(\mathbb{Q}_p)$ for $p \neq 2$ (with respect to the standard form).

Notice $O_3(\mathbb{Z}[p^{-1}]) \leq O_3(\mathbb{R}) \times O_3(\mathbb{Q}_p)$ discretely. But $O_3(\mathbb{R})$ is compact (notice that $O_3(\mathbb{R}, J)$ is not compact, this is why we work with the standard form), which implies $O_3(\mathbb{Z}[p^{-1}])$ is a discrete subgroup of $O_3(\mathbb{Q}_p)$! There are a few ways to see this point-topological argument, try thinking about this. Thus we can take $\Gamma(N) = \{\gamma \in O_3(\mathbb{Z}[p^{-1}]) : \gamma \equiv I \ (N)\}$, and $X^{p,N} = \Gamma(N)\backslash T_{p+1} = \Gamma(N)\backslash O_3(\mathbb{Q}_p)/O_3(\mathbb{Z}_p)$ is a finite graph, because $O_3(\mathbb{Z}[p^{-1}])\backslash O_3(\mathbb{Q}_p)$ is compact (not trivial!).

Fact (Lubotzky, Phillips, Sarnak): These are Ramanujan graphs, i.e. have optimal expansion. This requires *heavy* number theory (Deligne). To this day, these are the *only explicit constructions* of Ramanujan graphs. LPS also showed that if $p \equiv 1 \ (4)$, $X^{p,4q}$ can be described as a Cayley graph of the finite group $O_3(\mathbb{F}_q)$, where q is a prime. This is due to the fact $\Gamma(4)$ acts simply transitively on vertices.

8 Strong Approximation - Crash Course

Recall we defined the Adele ring $\mathbb{A} = \prod'_{p\leq\infty}\mathbb{Q}_p = \{(\alpha_\infty, \alpha_2, \alpha_3, \alpha_5, \dots) : \alpha_p \in \mathbb{Z}_p \text{ in some tail}\}$, and $\mathbb{Q}_\infty = \mathbb{R}$. This ring was useful when thinking about characters of $\mathbb{Q}$. We consider the *finite Adele ring*, $A_f = \prod'_{p<\infty}\mathbb{Q}_p$, i.e. we just forget about the real element in the sequence. This ring has two important subrings: $\mathbb{Q} \hookrightarrow \mathbb{A}_f$ diagonally, i.e. $r \mapsto (r, r, r, \dots)$, and the *integral Adele ring* $\hat{\mathbb{Z}} := \prod_{p<\infty}\mathbb{Z}_p \leq \mathbb{A}_f$. The latter is in fact a maximal compact subring of $\mathbb{A}_f$. What are the invertible elements in that ring? $\hat{\mathbb{Z}}^\times = \prod \mathbb{Z}_p^\times = \{(\alpha_p) : \text{val}(\alpha_p) = 0\ \forall p\}$.

What happens when we play the standard game of dividing out by a maximal compact subgroup? Take $G = \text{GL}_1$. We then have:

$$G(\mathbb{A}_f)/G(\hat{\mathbb{Z}}) = \mathbb{A}_f^\times/\hat{\mathbb{Z}}^\times = \prod{}'\,\mathbb{Q}_p^\times \,/ \prod \mathbb{Z}_p^\times = \prod{}'\,\mathbb{Q}_p^\times\,/\,\mathbb{Z}_p^\times = \prod{}'\,\mathbb{Z} = \bigoplus_p \mathbb{Z}$$

The penultimate equality comes from the valuation map.

Claim. $\mathbb{Q}^\times\hat{\mathbb{Z}}^\times = \mathbb{A}_f^\times$.

Using this claim, using the second isomorphism theorem:

$$G(\mathbb{A}_f)/G(\hat{\mathbb{Z}}) = \mathbb{A}_f^\times/\hat{\mathbb{Z}}^\times = \mathbb{Q}^\times\hat{\mathbb{Z}}^\times/\hat{\mathbb{Z}}^\times \cong \mathbb{Q}^\times \,/\left(\mathbb{Q}^\times \cap \hat{\mathbb{Z}}^\times\right) = \mathbb{Q}^\times/\{\pm 1\}$$

Convince yourself that the intersection is indeed $\{\pm 1\}$. We now conclude that a rational, up to a sign, is described by a choice of an integer at every prime, i.e. its valuation at that prime. This makes sense, and it is in fact just a very fancy way of saying $\mathbb{Q}$ has unique factorization (though we will use it in the proof of the claim, so we didn't even prove it). When we do this for GL_2, we *will* learn new things.

Proof of the claim (sketch). Given $\alpha \in \mathbb{A}_f^\times = \{(\alpha_p) : \alpha_p \neq 0, \text{val}(\alpha_p) = 0 \text{ in some tail}\}$, there exists some $r \in \mathbb{Q}^\times$ with $r\alpha \in \hat{\mathbb{Z}}^\times$, and the claim follows. □

Our goal is to do the same for $G = \text{PGL}_n$, i.e. to see that $G(\mathbb{Q})G(\hat{\mathbb{Z}}) = G(\mathbb{A}_f)$. This is what's called *strong approximation*, and we will prove it later. It is also easy to see that $G(\mathbb{Q}) \cap G(\hat{\mathbb{Z}}) = G(\mathbb{Z})$.

What do we learn from strong approximation? Again, using the second isomorphism theorem:

$$G(\mathbb{A}_f)/G(\hat{\mathbb{Z}}) = G(\mathbb{Q})/G(\mathbb{Z}) = \{\text{rational lattices up to } \mathbb{Q}\text{-scaling}\}$$

Thus we'll learn about the space of rational lattices. But:

$$\begin{aligned}&G(\mathbb{A}_f)/G(\hat{\mathbb{Z}}) = G\left(\prod{}'\,\mathbb{Q}_p\right)/G\left(\prod \mathbb{Z}_p\right) = \\ &\prod{}'\,G(\mathbb{Q}_p)/G(\mathbb{Z}_p) = \prod{}'\,\mathcal{B}_{n,p}^0 = \{(v_2, v_3, v_5, \dots) : v_p \in \mathcal{B}_{n,p}, v_p \text{ is the root in some tail}\}\end{aligned}$$

Which is an extremely interesting and useful result.

What happens if we add $\mathbb{R}$, i.e. consider $\mathbb{A}$ instead? We need to consider a slightly different object, similar to what we studied earlier, in the sense that $\mathbb{Q}$ is indeed discrete in $\mathbb{A}$. Let I_∞ be the identity at infinity and 0 elsewhere. Using strong approximation, we obtain:

$$\begin{aligned}&G(\mathbb{Q})\backslash G(\mathbb{A})/\left(I_\infty \times G(\hat{\mathbb{Z}})\right) = G(\mathbb{Q})\backslash\left(G(\mathbb{A}_f)/G(\hat{\mathbb{Z}}) \times G(\mathbb{R})\right) = G(\mathbb{Q})\backslash\left(\prod{}'\,\mathcal{B}_{n,p}^0 \times G(\mathbb{R})\right) = \\ &G(\mathbb{Q})\backslash\left(G(\mathbb{Q})/G(\mathbb{Z}) \times G(\mathbb{R})\right) \cong G(\mathbb{Z})\backslash G(\mathbb{R})\end{aligned}$$

This is the collection of real lattices up to homotethy! We thus get structure on this collection, through what's called the *Hecke neighbors*, i.e. starting with a lattice, going to neighbors of it in the restricted product representation above, and going back.

Lastly, we note that these results are most useful when talking about function spaces:

$$L^2\left(G(\mathbb{Q})\backslash\left({\prod}'\mathcal{B}^0_{p,n}\times G(\mathbb{R})\right)\right)\cong L^2\left(G(\mathbb{Z})\backslash G(\mathbb{R})\right)$$

Proof of strong approximation. Recall $\mathbb{Q}^\times\hat{\mathbb{Z}}^\times=\mathbb{A}_f^\times$. It is similar to prove $\mathbb{Q}+\hat{\mathbb{Z}}=\mathbb{A}_f$. However, $\mathbb{Q}$ is dense in $\mathbb{A}_f$ while $\mathbb{Q}^\times$ is not dense in $\mathbb{A}_f^\times$ (e.g. for $U=5\hat{\mathbb{Z}}+1\leq\hat{\mathbb{Z}}^\times$ we have $\mathbb{Q}^\times U<\mathbb{A}_f^\times$ strictly; this is left as an exercise). We show $\mathbb{Q}$ is dense in $\mathbb{A}_f$. Let $0\neq\alpha\in\mathbb{A}_f$. Then there exists $0\neq m\in\mathbb{N}$ such that $m\alpha\in\hat{\mathbb{Z}}$. We soon show $\mathbb{Z}$ is dense in $\hat{\mathbb{Z}}$, so there exists some $a_n\in\mathbb{Z}$ such that $a_n\to m\alpha$, so that $a_n/m\to\alpha$. Indeed, let $\alpha=(\alpha_2,\alpha_3,\alpha_5,\dots)\in\hat{\mathbb{Z}}$. Write these one above each other and draw a northwest-southeast diagonal. Then by the CRT there exists some $a\in\mathbb{N}$ which is compatible with these in every $\mathbb{Z}_p$. This shows $\mathbb{Z}$ is dense in $\hat{\mathbb{Z}}$.

We now show $\mathrm{SL}_n(\mathbb{Q})$ is dense in $\mathrm{SL}_n(\mathbb{A}_f)$. Start with $n=2$. It is easy to see that, for any p,

$$\overline{\mathrm{SL}_n(\mathbb{Q})}\geq\overline{\begin{pmatrix}1&\mathbb{Q}\\&1\end{pmatrix}}=\begin{pmatrix}1&\overline{\mathbb{Q}}\\&1\end{pmatrix}=\begin{pmatrix}1&\mathbb{A}_f\\&1\end{pmatrix}\supseteq\begin{pmatrix}1&\mathbb{Q}_p\\&1\end{pmatrix}$$

The same argument shows $\overline{\mathrm{SL}_2(\mathbb{Q})}$ contains the transpose of that. Now, for any field F,

$$\left\langle\begin{pmatrix}1&F\\&1\end{pmatrix},\begin{pmatrix}1&\\F&1\end{pmatrix}\right\rangle=\mathrm{SL}_2(F)$$

This means that for any p, $\overline{\mathrm{SL}_2(\mathbb{Q})}\supseteq\mathrm{SL}_2(\mathbb{Q}_p)$ (as the product $I\times\cdots\times I\times\mathrm{SL}_2(\mathbb{Q}_p)\times I\times\cdots$), so that for any P, $\overline{\mathrm{SL}_2(\mathbb{Q})}\supseteq\prod_{p\leq P}\mathrm{SL}_2(\mathbb{Q}_p)$. Taking closures, we get precisely the topology on $\mathrm{SL}_2(\mathbb{A}_f)$. This will work whenever G is generated by copies of the additive group. The proof for SL_n is thus the same (putting copies of F wherever we need). We can also do it for Sp_{2n},O_{2n}. In all these cases, $\overline{G(\mathbb{Q})}=G(\mathbb{A}_f)$. The general strong approximation theorem states that for G semi-simple/reductive, this is actually equivalent to $G(\mathbb{R})$ being non-compact and G being simply connected.

Recall we want to see that for $G=\mathrm{GL}_n$ we have $G(\mathbb{Q})G(\hat{\mathbb{Z}})=G(\mathbb{A}_f)$. It is not true that $G(\mathbb{Q})$ is dense in $G(\mathbb{A}_f)$. Note that $G(\mathbb{Q})G(\hat{\mathbb{Z}})\supseteq\mathrm{SL}_n(\mathbb{Q})\,\mathrm{SL}_n(\hat{\mathbb{Z}})=\mathrm{SL}_n(\mathbb{A}_f)$, since $\mathrm{SL}_n(\hat{\mathbb{Z}})$ is open and we saw $\mathrm{SL}_n(\mathbb{Q})$ is dense. Thus $\mathrm{SL}_n(\mathbb{A}_f)\leq G(\mathbb{Q})G(\hat{\mathbb{Z}})\leq\mathrm{GL}_n(\mathbb{A}_f)$. We claim that the latter containment is an equality. By the correspondence theorem, $G(\mathbb{Q})G(\hat{\mathbb{Z}})$ corresponds to a subgroup of the quotient $\mathrm{GL}_n(\mathbb{A}_f)/\,\mathrm{SL}_n(\mathbb{A}_f)$, which is precisely $\mathbb{A}_f^\times$ via the determinant map. Thus we wish to find the image of $G(\mathbb{Q})G(\hat{\mathbb{Z}})$ under the determinant map. All that is left to show is thus that $\det\left(G(\mathbb{Q})G(\hat{\mathbb{Z}})\right)=\mathbb{A}_f^\times$. But indeed this is precisely $\det(G(\mathbb{Q}))\det\left(G(\hat{\mathbb{Z}})\right)=\mathbb{Q}^\times\hat{\mathbb{Z}}^\times=\mathbb{A}_f^\times$, so we're done. □

This concludes our course.

p-adic groups - Exercise 1

This is a long exercise - I think doing $\frac{2}{3}$ of the questions is more than enough.

1. (a) Prove that $\mathbb{Q}_9 \cong \mathbb{Q}_3$ (write an explicit isomorphism).
   (b) Prove that $\mathbb{Z}_{10} \cong \mathbb{Z}_2 \times \mathbb{Z}_5$, and $\mathbb{Q}_{10} \cong \mathbb{Q}_2 \times \mathbb{Q}_5$. Can you write an explicit isomorphisms?

2. Let p be a prime. Let $\alpha \in \mathbb{Q}_p$, and write $\alpha = p^m u$ with $m \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$.
   (a) For $p \neq 2$, prove that α has a square root in $\mathbb{Q}_p$ iff $m \in 2\mathbb{Z}$, and $(u \bmod p)$ has a square root in $\mathbb{F}_p$.
   (b) For $p = 2$, prove that α has a square root in $\mathbb{Q}_2$ iff $m \in 2\mathbb{Z}$, and $u \equiv 1 \pmod 8$.
   Hint: Hensel's Lemma does not work directly, so you need to make some variation. You can work out the specific case given here, and you can look for a stronger version of Hensel's Lemma in literature/online and use it (and you are encouraged to prove it).

3. Prove that $\alpha \in \mathbb{Q}_p$ is in $\mathbb{Q}$ iff it is periodic. Tip: recall first how you proved this in $\mathbb{R}$.

4. Recall that the polynomial $x^n - 1$ is separable over every field $\mathbb{F}$ of characteristic zero, so $\overline{\mathbb{F}}$ always has n n^{th}-roots of unity, which are denoted μ_n. Let $p \neq 2$, and show that:
   (a) $\mathbb{Q}_p$ has all the $(p-1)$-roots of unity.
   (b) $(1 + p\mathbb{Z}_p) \leq \mathbb{Z}_p^\times$, and $\mathbb{Z}_p^\times = (1 + p\mathbb{Z}_p) \times \mu_{p-1}$ as a group (where μ_{p-1} are the $(p-1)$ roots of unity in $\mathbb{Q}_p$).
   (c) exp and log give an isomorphism $(p\mathbb{Z}_p, +) \cong (1 + p\mathbb{Z}_p, \times)$. (They are defined by their power series, $\exp \alpha = \sum_{k=0}^{\infty} \frac{\alpha^k}{k!}$ and $\log(1+\alpha) = -\sum_{k=1}^{\infty} \frac{(-x)^k}{k}$. The main issue is to show convergence, the fact that they are inverse to one another follows from formal power series wizardry).
   (d) Combine everything to show that $\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}_p^+ \times \mathbb{Z}/(p-1)\mathbb{Z}$. (namely, the multiplicative group of $\mathbb{Q}_p$ can be described by the additive group. In the real case you have $\mathbb{R}^\times \cong \mathbb{R}^+ \times \mathbb{Z}/2\mathbb{Z}$ similarly).
   (e) Do everything for $p = 2$ - there are differences in every step, and you should get $\mathbb{Q}_2^\times \cong \mathbb{Z} \times \mathbb{Z}_2^+ \times \mathbb{Z}/2\mathbb{Z}$ at the end.

5. Let q be a prime. Recall that for every $\ell \in \mathbb{N}$ there is a unique field $\mathbb{F}_{q^\ell}$ of size q^ℓ, and $\mathbb{F}_{q^\ell}$ embeds in $\mathbb{F}_{q^k}$ iff $\ell \mid k$. Recall also that $\mathbb{F}_{q^\ell}/\mathbb{F}_q$ is a cyclic Galois extension, whose Galois group is generated by the "Frobenius automorphism" $\phi(x) = x^q$.
   (a) Let p be any prime (possibly $p = q$), and observe the ascending chain of fields

$$\mathbb{F}_q \subset \mathbb{F}_{q^p} \subset \mathbb{F}_{q^{p^2}} \subset \mathbb{F}_{q^{p^3}} \subset \dots$$

   Convince yourself that the union $\mathbb{F} = \bigcup_{m=1}^{\infty} \mathbb{F}_{q^{(p^m)}}$ is a field, and show that $\mathrm{Aut}(\mathbb{F}/\mathbb{F}_q) \cong \mathbb{Z}_p$ (write an explicit isomorphism).

(b) Convince yourself that every $m \in \mathbb{N}$ has a unique representation as $m = \sum_{j=1}^{n} d_j j!$ with $n \in \mathbb{N}$ and $0 \leq d_j \leq j!$. It is useful to think about this as writing m in a basis where every decimal place has a different "value" (This is a real thing - see Wikipedia article "factorial number system", and `https://www.dcode.fr/factorial-base`). Define the *factoradic integers* $\mathbb{Z}_!$ to be the left-infinite version of these numbers:

$$\mathbb{Z}_! = \left\{ \sum_{j=1}^{\infty} d_j j! \,\middle|\, \forall j : 0 \leq d_j \leq j! \right\}$$

with addition and multiplication extending that of $\mathbb{N}$.[1] Show that if

$$\mathbb{F} = \bigcup_{m=1}^{\infty} \mathbb{F}_{q^{n!}}$$

then $\operatorname{Aut}\left(\mathbb{F}/\mathbb{F}_q\right) \cong \mathbb{Z}_!$

(c) Show that $\mathbb{F} = \bigcup_{n=1}^{\infty} \mathbb{F}_{q^{n!}}$ is an algebraic closure of $\mathbb{F}_q$ (so we got $\operatorname{Aut}\left(\overline{\mathbb{F}_q}/\mathbb{F}_q\right) \cong \mathbb{Z}_!$. Can you find a nice description for $\operatorname{Aut}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$?)

6. (a) Show that $x^2 + 1$ is irreducible in $\mathbb{Q}_3[x]$, so that $\mathbb{Q}_3[i] := {}^{\mathbb{Q}_3[x]}/_{(x^2+1)}$ is a quadratic field extension of $\mathbb{Q}_3$.

(b) Show that $3 \cdot \mathbb{Z}_3[i]$ is a maximal ideal in $\mathbb{Z}_3[i]$, with ${}^{\mathbb{Z}_3[i]}/_{3\mathbb{Z}_3[i]} \cong \mathbb{F}_9$. Tip: consider also $\left({}^{\mathbb{Z}}/_{3\mathbb{Z}}\right)[i]$.

(c) Show that every $0 \neq \alpha \in \mathbb{Q}_3[i]$ can be written uniquely as $\alpha = 3^m u$ with $m \in \mathbb{Z}$ and $u \in \mathbb{Z}_3[i]^{\times}$.

[1] If you prefer, you can think of an inverse limit, $\mathbb{Z}_! = \varprojlim {}^{\mathbb{Z}}/_{(n!)} = \left\{ \vec{a} \in \prod_{n=1}^{\infty} {}^{\mathbb{Z}}/_{n!} \,\middle|\, \forall i : a_{i+1} \equiv a_i \pmod{i!} \right\}$.

p-adic groups - Exercise 2

1. Fourier 101: Let G be a finite cyclic group (or finite abelian, if you dare), and $\widehat{G} = \mathrm{Hom}\left(G, \mathbb{C}^\times\right)$. We regard $\mathbb{C}^G$ as an inner-product space with the normalized inner-product
$$\left\langle f, f' \right\rangle := \frac{1}{|G|} \sum_{g \in G} f\left(g\right) \overline{f'\left(g\right)}.$$
For $f \colon G \to \mathbb{C}$, we define its *Fourier transform* $\hat{f} \colon \widehat{G} \to \mathbb{C}$ by $\hat{f}\left(\chi\right) := \langle f, \chi \rangle$.

   (a) Show that $\widehat{G}$ is an orthonormal basis for $\mathbb{C}^G$, and deduce that $f = \sum_\chi \hat{f}\left(\chi\right)\chi$.

   (b) Show that $\widehat{f * g}\left(\chi\right) = \hat{f}\left(\chi\right)\hat{g}\left(\chi\right)$, where $*$ is the normalized convolution operator
$$\left(f * f'\right)\left(g\right) = \frac{1}{|G|} \sum_{h \in G} f\left(gh^{-1}\right) f'\left(h\right).$$
(if you know what $\mathbb{C}\left[G\right]$ is, this shows that $\mathbb{C}\left[G\right] \cong \mathbb{C}^{|G|}$ as rings).

   (c) For $g \in G$, we define $ev_g \colon \widehat{G} \to \mathbb{C}^\times$ by $ev_g\left(\chi\right) := \chi\left(g\right)$ ("evaluation at g"). Show that $g \mapsto ev_g$ gives an isomorphism $G \cong \widehat{\widehat{G}}$.

   (d) Prove the Fourier Inversion Theorem: $\hat{\hat{f}}(ev_g) = \frac{1}{|G|} f\left(g^{-1}\right)$.

2. (a) Show that $\widehat{\mathbb{Z}_p} \cong {}^{\mathbb{Z}[1/p]}/_{\mathbb{Z}}$ (we showed in class that $\widehat{{}^{\mathbb{Z}[1/p]}/_{\mathbb{Z}}} \cong \mathbb{Z}_p$, but please do not resort to Pontryagin duality, we are not animals).

   (b) Show that $\widehat{\mathbb{Z}\left[1/p\right]} \cong {}^{(\mathbb{Q}_p \times \mathbb{R})}/_{\{(r,r) \,|\, r \in \mathbb{Z}[1/p]\}}$, when we consider $\mathbb{Z}\left[1/p\right]$ with discrete topology.

3. Let $G = \left(\begin{smallmatrix} \mathbb{Q}_p^\times & \mathbb{Q}_p \\ 0 & 1 \end{smallmatrix}\right) \leq GL_2\left(\mathbb{Q}_p\right)$ and let μ be the left Haar measure of G, normalized so that $\mu\left(K\right) = 1$ for $K = \left(\begin{smallmatrix} \mathbb{Z}_p^\times & \mathbb{Z}_p \\ 0 & 1 \end{smallmatrix}\right)$. Show that $\mu\left(K\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)\right) \neq 1$ and conclude that μ is *not* a right Haar measure (namely, G is not *unimodular*). Hint: there is no need to describe μ – you only need it being left-invariant (so that $\mu\left(gK\right) = 1$ for any $g \in G$), and additive on disjoint unions.

4. This is another analogy between the symmetric spaces of real and p-adics GL_n:

   (a) Recall that
$$O(n) = \{g \in GL_n\left(\mathbb{R}\right) \,|\, \forall v \in \mathbb{R}^n : \|gv\| = \|v\|\}$$
was a maximal compact subgroup of $GL_n\left(\mathbb{R}\right)$, while $GL_n\left(\mathbb{Z}_p\right)$ was a max. cpt. of $GL_n\left(\mathbb{Q}_p\right)$. Prove that if we define $\|v\|_p = \max_{i=1}^n |v_i|_p$ for $v \in \mathbb{Q}_p^n$, then
$$GL_n\left(\mathbb{Z}_p\right) = \left\{g \in GL_n\left(\mathbb{Q}_p\right) \,\middle|\, \forall v \in \mathbb{Q}_p^n : \|gv\|_p = \|v\|_p\right\}.$$

(b) More generally, say that $N\colon \mathbb{Q}_p^n \to p^{\mathbb{Z}} \cup \{0\}$ is a *norm* if

i. $N(v) = 0 \Rightarrow v = 0$.

ii. $N(\alpha v) = |\alpha|_p N(v)$ for any $\alpha \in \mathbb{Q}_p$.

iii. $N(v+w) \leq \max(N(v), N(w))$.

Show that $GL_n(\mathbb{Q}_p)$ acts transitively on the set of all norms (by $(gN)(v) = N(gv)$). A possible direction (there are other ways to prove this!): show that the unit ball (w.r.t. N) is an open $\mathbb{Z}_p$-submodule of $\mathbb{Q}_p^n$,[1] and that a bounded open $\mathbb{Z}_p$-submodule of $\mathbb{Q}_p^n$ is a $\mathbb{Z}_p$-lattice.

Combining (a) and (b), we find that $GL_n(\mathbb{Q}_p)/GL_n(\mathbb{Z}_p)$ can be identified with the space of all norms on $\mathbb{Q}_p^n$ (over $\mathbb{R}$ we have that $GL_n(\mathbb{R})/O(n)$ is the space of all inner products on $\mathbb{R}^n$ – you are encouraged to finish the proof we started in class).

5. Show every coset in ${}^{PGL_d(\mathbb{Q}_p)}\!/\!{}_{PGL_d(\mathbb{Z}_p)}$ has a unique representative of the form

$$A = \begin{pmatrix} p^{m_1} & b_{12} & b_{13} & \cdots & b_{1d} \\ & p^{m_2} & b_{23} & \cdots & b_{2d} \\ & & \ddots & & \vdots \\ & 0 & & p^{m_{d-1}} & b_{d-1,d} \\ & & & & p^{m_d} \end{pmatrix} \in M_d(\mathbb{Z})$$

with each $0 \leq b_{ij} < p^{m_i}$, and $\frac{A}{p} \notin M_d(\mathbb{Z})$.

6. Prove the Cartan decomposition over $\mathbb{Q}_p$:

$$PGL_d(\mathbb{Q}_p) = \bigsqcup_{0=m_1\leq m_2\leq\ldots\leq m_d} PGL_d(\mathbb{Z}_p)\operatorname{diag}(p^{m_1},\ldots,p^{m_d})\,PGL_d(\mathbb{Z}_p).$$

7. In this question $\mathcal{B}_2$ is the Bruhat-Tits tree of $G = PGL_2(\mathbb{Q}_p)$, and v_0 is the vertex with stabilizer $K = PGL_2(\mathbb{Z}_p)$.

(a) For $g \in GL_2(\mathbb{Q}_p)$, show that

$$\operatorname{dist}_{\mathcal{B}_2}(v_0, gv_0) = \operatorname{val}_p(\det g) - 2\min_{i,j}\operatorname{val}_p(g_{i,j}).$$

(b) Show that the stabilizer of the path from v_0 to $\begin{bmatrix} 1 & \\ & p^\ell \end{bmatrix}$ is $\begin{pmatrix} \mathbb{Z}_p^\times & \mathbb{Z}_p \\ p^\ell\mathbb{Z}_p & \mathbb{Z}_p^\times \end{pmatrix}$.

(c) Show that K does not act 2-transitively on any sphere in the tree except for the first one.

(d) Show that $PGL_2(\mathbb{F}_p)$ acts sharply 3-transitively on $\mathbb{P}^1\mathbb{F}_p$, the projective line over $\mathbb{F}_p$. You can think of $\mathbb{P}^1\mathbb{F}_p$ either as $\mathbb{F}_p \cup \{\infty\}$ with $PGL_2(\mathbb{F}_p)$ acting by Möbius transformations, or as the lines in $\mathbb{F}_p^2$, with $PGL_2(\mathbb{F}_p)$ acting as linear transformations.

[1] in case you never saw modules: a $\mathbb{Z}_p$-submodule of $\mathbb{Q}_p^n$ is simply a subset of $\mathbb{Q}_p^n$ which is closed under addition, and under multiplication by scalars from $\mathbb{Z}_p$.

p-adic groups - Exercise 3

1. (Bruhat decomposition) Let $\mathbb{F}$ be any field, $G = GL_d(\mathbb{F})$ and $P \leq G$ the upper triangular matrices.
   (a) Prove that $G = \bigcup_{\pi \in S_d} P\pi P$. (Hint: use P for column and row operations)
   (b) Prove that this is a disjoint union, i.e. S_d is a transversal for $P \backslash G / P$. Hint: show first that if $\pi p \pi' \in P$ for $\pi, \pi' \in S_d$ then $\pi' = \pi^{-1}$.

From here $G = PGL_d(\mathbb{Q}_p), v_0, K, \sigma_0, B, A^+, A, \mathcal{A}_0, W$ are as defined in class.

2. Show that $G = \bigsqcup_{w \in W} BwB$ (we proved $G = \bigcup_{w \in W} BwB$ in class).

3. Denote by M the monomial matrices in G (matrices with entries on a generalized diagonal)
   (a) Prove that $\mathrm{Stab}^{pw}(\mathcal{A}_0) = \begin{pmatrix} \mathbb{Z}_p^\times & & \\ & \ddots & \\ & & \mathbb{Z}_p^\times \end{pmatrix}$.
   (b) Prove that $M = N_G(A) = \mathrm{Stab}^{sw}(\mathcal{A}_0)$, and that $W \cong {}^{\mathrm{Stab}^{sw}(\mathcal{A}_0)}/_{\mathrm{Stab}^{pw}(\mathcal{A}_0)}$.

4. For $v, w \in X_d^0$ we define $\mathrm{dist}(v, w)$ as the length of the shortest path in X_d between v and w (by path we mean a path through edges, and the length is the number of edges). We also define $\mathrm{dist}_1(v, w)$ as the length of the shortest path in X_d **from** v **to** w made of edges **of color one**.
   (c) Prove that if $v \in \mathcal{A}_0$ then there is a path of length $\mathrm{dist}(v_0, v)$ from v_0 to v which is contained in $\mathcal{A}_0$. Do the same for $\mathrm{dist}_1(v_0, v)$.
   (d) Check that $\mathrm{dist}_1\left(v_0, \begin{bmatrix} 1 & & \\ & 1 & \\ & & p \end{bmatrix}\right) = 1$ while $\mathrm{dist}_1\left(\begin{bmatrix} 1 & & \\ & 1 & \\ & & p \end{bmatrix}, v_0\right) = 2$, so dist_1 is not symmetric.
   (e) Let $g \in KaK$ with $a \in A^+$. Show that $\mathrm{dist}(v_0, gv_0) = \mathrm{dist}(v_0, av_0)$ and $\mathrm{dist}_1(v_0, gv_0) = \mathrm{dist}_1(v_0, av_0)$.
   (f) Show that if $a = \mathrm{diag}(p^{m_1}, p^{m_2}, \ldots, p^{m_d})$ (with $0 = m_1 \leq m_2 \leq \ldots$) then
   $$\mathrm{dist}_1(v_0, av_0) = \sum\nolimits_{j=1}^{d} m_j \qquad \text{and} \qquad \mathrm{dist}(v_0, av_0) = m_d.$$
   (g) For $g \in GL_d(\mathbb{Q}_p)$ define
   $$\ell(g) = \mathrm{val}_p(\det g) - d \min_{i,j} \mathrm{val}_p(g_{i,j})$$
   (and observe that ℓ is well defined on $PGL_d(\mathbb{Q}_p)$). Show that $\mathrm{dist}_1(v_0, gv_0) = \ell(g)$. Tip: prove that ℓ is K-bi-invariant (i.e. $\ell(kg) = \ell(g) = \ell(gk)$ for $k \in K$), and note that so is $g \mapsto \mathrm{dist}_1(v_0, gv_0)$.
   (h) Show that $\mathrm{dist}(v_0, gv_0) = \frac{\ell(g) + \ell(g^{-1})}{d}$.

p-adic groups - Final exercise

The work on this exercise should be individual. If you are stuck you can consult with me.
Each sub-question is worth 10 points, up to a maximum of 100.

1. Let $p \neq 2$. In this question we will show that $O_3\left(\mathbb{Q}_p, \begin{pmatrix}1&&\\&1&\\&&1\end{pmatrix}\right) \cong O_3\left(\mathbb{Q}_p, \begin{pmatrix}&&1\\&1&\\1&&\end{pmatrix}\right)$. We denote by $\langle\ ,\ \rangle$ the standard bilinear form on $\mathbb{Q}_p^3$.
   (a) Show there exist $a, b \in \mathbb{F}_p$ with $a^2 + b^2 = -1$.
   (b) Show there exists $0 \neq v \in \mathbb{Z}_p^3$ with $\langle v, v\rangle = 0$. Hint: start with $a, b \in \mathbb{Z}_p$ such that $a^2 + b^2 = -1 \pmod p$, and find c such that $a^2 + b^2 + c^2 = 0$.
   (c) Show there exists $w \in \mathbb{Q}_p^3$ such that $\langle v, w\rangle = 1$ and $\langle w, w\rangle = 0$.[1]
   (d) Show there exists $u \in \mathbb{Q}_p^3$ such that $\langle u, v\rangle = \langle u, w\rangle = 0$, and $\langle u, u\rangle \neq 0$. Denoting $\varepsilon = \langle u, u\rangle$, show that $\langle\ ,\ \rangle$ is represented in the basis $\{v, u, w\}$ by the matrix $\begin{pmatrix}&&1\\&\varepsilon&\\1&&\end{pmatrix}$.
   (e) Show there is a basis in which $\langle\ ,\ \rangle$ is represented by $\begin{pmatrix}&&\varepsilon\\&\varepsilon&\\\varepsilon&&\end{pmatrix}$, and conclude that $O_3\left(\mathbb{Q}_p, \begin{pmatrix}1&&\\&1&\\&&1\end{pmatrix}\right) \cong O_3\left(\mathbb{Q}_p, \begin{pmatrix}&&1\\&1&\\1&&\end{pmatrix}\right)$.

2. Let $K \leq GL_n(\mathbb{Q}_p)$ be a compact subgroup.
   (a) For $L_0 = \mathbb{Z}_p^n$ the standard $\mathbb{Z}_p$-lattice, show that $\{kL_0 \mid k \in K\}$ is a finite set (of $\mathbb{Z}_p$-lattices).
   (b) Show that a finite sum of $\mathbb{Z}_p$-lattices is a $\mathbb{Z}_p$-lattice, and that K stabilizes the $\mathbb{Z}_p$-lattice $\sum_{k\in K} kL_0$.
   (c) Show that every maximal compact subgroup of $GL_n(\mathbb{Q}_p)$ is a conjugate of $GL_n(\mathbb{Z}_p)$.
   (d) Find a compact subgroup of $PGL_2(\mathbb{Q}_p)$ which is **not** contained in any conjugate of $PGL_2(\mathbb{Z}_p)$.

3. Let $G = PGL_d(\mathbb{Q}_p)$, $K = PGL_d(\mathbb{Z}_p)$, and $\mathcal{B}$ the building of G (so that $\mathcal{B}^0 = {}^{G}\!/_{K}$ via $gv_0 \mapsto gK$). A *Hecke operator* on $\mathcal{B}$ is a map $T\colon \mathcal{B}^0 \to \left\{\substack{\text{finite subsets}\\ \text{of } \mathcal{B}^0}\right\}$ which commutes with G. Namely, for every vertex $v \in \mathcal{B}^0$, $T(v)$ is a finite set of vertices, and $T(gv) = gT(v)$ for any $g \in G$. For example, the adjacency operator (sending v to its neighbors in the tree/building) is a Hecke operator.
   (a) Show that a Hecke operator T is determined by $T(v_0)$, and that $T(v_0)$ is a K-stable set of vertices. On the other hand, show that any finite K-stable set S of vertices determines a (unique) Hecke operator T such that $T(v_0) = S$.
   (b) For a double coset KxK ($x \in G$), show that $T_x(gv_0) := gKxv_0$ (for $g \in G$) is a well defined Hecke operator (and does not depend on the representative x for the double coset).
   (c) Show that every Hecke operator can be written as a union of operators of the form T_x ($x \in G$).
   (d) Show that for $x, y \in G$ the operators T_x, T_y commute, and conclude that all Hecke operators on $\mathcal{B}$ commute with each other. Hint: show that $KxKyK = KyKxK$.
   (e) (challenge) Let $x_i = \operatorname{diag}\Bigg(1, \ldots, 1, \underbrace{p, \ldots, p}_{i \text{ times}}\Bigg)$. Show that the Hecke operators $T_{x_0}, \ldots, T_{x_{d-1}}$ generate together all the Hecke operators on $\mathcal{B}$ (via composition, union and subtraction).

[1] A pair of vectors v, w satisfying $\langle v, v\rangle = \langle w, w\rangle = 0$ and $\langle v, w\rangle = 1$ are called a *hyperbolic pair*.