p-adic numbers and Diophantine equations

Yuri Bilu

Fall semester 2013

These are notes from a class given by Yuri Bilu at Universié de Bordeaux in Fall semester 2013, TEX'ed by Lyosha Beshenov.

Version 2014-09-29. Corrections and remarks from Gabriel Chicas Reyes, Pietro Gatti, Roberto Gualdi, José Ibrahim Villanueva Gutiérrez. I try to keep this text updated. Please write about misprints and mistakes to

alexey.beshenov@math.u-bordeaux.fr

The latest edition is available at

http://www.math.u-bordeaux.fr/~abesheno/

Contents

Part I
Hasse–Minkowski theorem

1 Introduction to the p-adic integers $\mathbb{Z}_p$

Our motivation is the *local study of Diophantine equations.* A **Diophantine equation** has form $F(X_1,\dots,X_n)=0$ for some $F(X_1,\dots,X_n)\in\mathbb{Z}[X_1,\dots,X_n]$, and we are interested in its integral solutions $(x_1,\dots,x_n)\in\mathbb{Z}^n$. Assume we have such a solution. Then trivially the following holds:

1. The equation $F(X_1,\dots,X_n)=0$ has a real solution $\underline{x}\in\mathbb{R}^n$.
2. For each $m=1,2,3,\dots$ the congruence $F(X_1,\dots,X_n)\equiv 0 \pmod m$ has a solution.

The question is whether the converse is true, i.e. do the two conditions above imply existence of a solution in $\mathbb{Z}^n$? In general the answer is **no**, even for equations in one variable.

Example 1.1. Consider an equation $(X^2-13)(X^2-17)(X^2-13\cdot 17)=0$. It obviously has a real root; further one can check that it has solutions modulo m for each m (*exercise*). As we see, there are still no integer solutions. ▲

Our goal is to show the following result.

Theorem 1.2 (Hasse, Minkowski)**.** *Let $F(X_1,\dots,X_n)\in\mathbb{Z}[X_1,\dots,X_n]$ be a quadratic form (i.e. a homogeneous polynomial of degree two). Assume that*

1. *The equation $F(X_1,\dots,X_n)=0$ has a nontrivial solution $\underline{x}\in\mathbb{R}^n$.*
2. *For each $m=1,2,3,\dots$ the equation $F(X_1,\dots,X_n)\equiv 0 \pmod m$ has a nontrivial solution.*

Then $F(X_1,\dots,X_n)=0$ has a nontrivial solution $\underline{x}\in\mathbb{Z}^n$.

Our proof of this result will be conceptual and elaborate. We start from recalling some basic facts and introducing the p-adic numbers.

Proposition 1.3 (Chinese remainder theorem)**.** *Let $m=m_1m_2$ with m_1 and m_2 relatively prime integers. A congruence $F(X)\equiv 0 \pmod m$ has a solution iff both congruences $F(X)\equiv 0 \pmod{m_1}$ and $F(X)\equiv 0 \pmod{m_2}$ have solutions.*

Recall that the statement above comes from a ring isomorphism

$$\begin{aligned}\mathbb{Z}/m\mathbb{Z}&\cong\mathbb{Z}/m_1\mathbb{Z}\times\mathbb{Z}/m_2\mathbb{Z},\\ x&\mapsto (x \bmod m_1,\ x \bmod m_2).\end{aligned}$$

So since every m is a product $p_1^{k_1}\cdots p_s^{k_s}$ of prime powers, it is enough to consider only congruences modulo p^k. And this is where the p-adic numbers come into play.

Example 1.4. Consider a congruence $X^2\equiv 2 \pmod{7^k}$ for $k=1,2,3,\dots$

- If $\underline{k=1}$, then the solutions are $x=\pm 3 \pmod 7$.
- If $\underline{k=2}$, then the equation is $X^2\equiv 2 \pmod{7^2}$, so that $x^2=7^2\cdot u+2$, and x should be also a solution of $X^2\equiv 2 \pmod 7$, that is $x\equiv\pm 3 \pmod 7$.

  Suppose $x\equiv x_0=3 \pmod 7$, so $x=7u+3$. We have

$$\begin{aligned}(7u+3)^2 &\equiv 2 \pmod{7^2},\\ 2\cdot 3\cdot 7u+9 &\equiv 2 \pmod{7^2},\\ 2\cdot 3\cdot 7u+7 &\equiv 0 \pmod{7^2},\\ 6u+1 &\equiv 0 \pmod{7}.\end{aligned}$$

So we conclude $u \equiv 1 \pmod 7$, and the corresponding solution of $X^2 \equiv 2 \pmod{7^2}$ is $x_1 = 7\cdot 1+3 = 10$.

- Proceeding as above for $\underline{k=3}$, we look for $x_2 = 7^2\cdot u + x_1$ such that $x_2^2 \equiv 2 \pmod{7^3}$.

$$\begin{aligned}(7^2\cdot u + x_1)^2 &\equiv 2 \pmod{7^3},\\ 2\cdot 7^2\cdot u\cdot x_1 + x_1^2 &\equiv 2 \pmod{7^3},\\ 2\cdot 7^2\cdot u\cdot 10 + 2\cdot 7^2 &\equiv 0 \pmod{7^3},\\ 20u+2 &\equiv 0 \pmod{7}.\end{aligned}$$

So we conclude $u = 2$ and $x_2 = 7^2\cdot 2+10 = 108$.

Continuing in this manner, we have a sequence of numbers x_k (with $k = 0,1,2,\ldots$) such that $x_k^2 \equiv 2 \pmod{7^{k+1}}$ and $x_k \equiv x_{k-1} \pmod{7^k}$. The sequence starts with $x_0 = 3$, $x_1 = 10$, $x_2 = 108$, … It looks like an approximation to $\sqrt{2}$ digit by digit, but it is not decimal, it is 7-adic! ▲

Definition 1.5. Let p be a prime number. We say that a sequence of integers $(x_0, x_1, x_2, \ldots)$ gives a **p-adic integer** if

$$x_n \equiv x_{n-1} \pmod{p^n} \text{ for every } n = 1,2,3,\ldots \qquad (*)$$

Further we say that two sequences $(x_0, x_1, x_2, \ldots)$ and $(x_0', x_1', x_2', \ldots)$ define the same p-adic integer if $x_n \equiv x_n' \pmod{p^{n+1}}$ for all $n = 0,1,2,\ldots$ We write $(x_n) \sim (x_n')$ in this case.

This is an equivalence relation, and the set of p-adic integers $\mathbb{Z}_p$ is defined to be the set of all integer sequences $(x_0, x_1, x_2, \ldots)$ satisfying (*), modulo this equivalence.

To each integer $x \in \mathbb{Z}$ corresponds a p-adic integer given by the sequence $(x, x, x, \ldots)$ (modulo the equivalence). This gives an embedding $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$.

Of course every p-adic integer can be defined by a sequence (x_n) where $x_n \in \{0,1,\ldots,p^{n+1}-1\}$. We call it a **canonical sequence**.

Now consider a sequence $(x_0, x_1, x_2, \ldots)$. We have $x_1 \equiv x_0 \pmod p$, so that $x_1 = x_0 + a_1 p$. If we assume that $0 \le x_0 < p$, then we have $0 \le a_1 \le p-1$. Proceeding in this manner,

$$\begin{aligned}x_1 &= a_0 + a_1 p,\\ x_2 &= a_0 + a_1 p + a_2 p^2,\\ &\cdots\\ x_n &= a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n,\\ &\cdots\end{aligned}$$

where $a_i \in \{0,1,\ldots,p-1\}$. This is called the **$p$-adic expansion** of $(x_0, x_1, x_2, \ldots)$, and it is unique.

Remark 1.6. Here is how one can calculate p-adic expansions in PARI/GP (http://pari.math.u-bordeaux.fr/):

```
? -1 + O(7^10)
%1 = 6 + 6*7 + 6*7^2 + 6*7^3 + 6*7^4 + 6*7^5 + 6*7^6 + 6*7^7 + 6*7^8 + 6*7^9 + O(7^10)

? sqrt(2+O(7^10))
%2 = 3 + 7 + 2*7^2 + 6*7^3 + 7^4 + 2*7^5 + 7^6 + 2*7^7 + 4*7^8 + 6*7^9 + O(7^10)
```

So every element of $\mathbb{Z}_p$ corresponds bijectively to a sequence $(a_0, a_1, a_2, \ldots)$ with $a_i \in \{0, 1, \ldots, p-1\}$. This set is really big, it has cardinality of the continuum.

The p-adic integers $\mathbb{Z}_p$ form a commutative ring. For two numbers $x = (x_n) \in \mathbb{Z}_p$ and $y = (y_n) \in \mathbb{Z}_p$ we define the sum and product by

$$x + y := (x_n + y_n), \quad x \cdot y := (x_n\, y_n).$$

One checks that this does not depend on the choice of sequences representing x and y.

Note that we define addition and multiplication for sequences and not for p-adic expansions. Adding and multiplying p-adic expansions is tricky: one should think about carrying digits, just like for the long multiplication of the usual integers written in, say, base ten.

Finally, we note that all the definitions above can be summarized as follows: $\mathbb{Z}_p$ is the inverse limit of rings $\mathbb{Z}/p^n\mathbb{Z}$:

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

Remark 1.7. The construction of p-adic integers can be generalized to the so-called **ring of Witt vectors**. For instance, $\mathbb{Z}_p$ is the ring of Witt vectors $W(\mathbb{F}_p)$ of the finite field $\mathbb{F}_p$. See *J.–P. Serre, Corps locaux, §II.6.*

Theorem 1.8. *A p-adic integer $x = (x_n)$ is invertible in $\mathbb{Z}_p$ iff x_0 is invertible modulo p, i.e. whenever $x_0 \not\equiv 0 \pmod p$.*

Proof. Assume x is invertible, so that $x\,y = 1$ for some $y \in \mathbb{Z}_p$. Then they are represented by sequences $x = (x_0, x_1, x_2, \ldots)$ and $y = (y_0, y_1, y_2, \ldots)$ such that $x_n\, y_n \equiv 1 \pmod{p^{n+1}}$. In particular, this means that $x_0 \not\equiv 0 \pmod p$.

In the opposite direction, assume that $x_0 \not\equiv 0 \pmod p$. We have $x_n \equiv x_{n-1} \pmod{p^n}$, and thus $x_n \equiv x_{n-1} \pmod p$,

$$x_n \equiv x_{n-1} \equiv x_{n-2} \equiv \cdots \equiv x_0 \not\equiv 0 \pmod p.$$

$x_n \not\equiv 0 \pmod p$ means that x_n is invertible $\pmod{p^{n+1}}$, so there exists y_n such that $x_n\, y_n \equiv 1 \pmod{p^{n+1}}$, meaning that $(x_n) \cdot (y_n) \sim 1$. We have to check that (y_n) gives a p-adic integer. Indeed,

$$\begin{gathered}
x_n\, y_n \equiv 1 \pmod{p^{n+1}}, \\
x_{n-1}\, y_{n-1} \equiv 1 \pmod{p^n}, \\
x_n \equiv x_{n-1} \pmod{p^n}, \\
x_{n-1}\, y_n \equiv x_{n-1}\, y_{n-1} \equiv 1 \pmod{p^n}, \\
y_n \equiv y_{n-1} \pmod{p^n}.
\end{gathered}$$

■

Corollary 1.9. *Every $x \in \mathbb{Z}$ is invertible in $\mathbb{Z}_p$ iff $x \not\equiv 0 \pmod p$.*

Example 1.10. 2 is invertible in $\mathbb{Z}_3$, so let us compute $\frac{1}{2} \in \mathbb{Z}_3$ as a sequence $(x_0, x_1, x_2, \ldots)$.

We should have $2\,x_0 \equiv 1 \pmod 3$, so $x_0 = 2$.

Then $2\,x_1 \equiv 1 \pmod{3^2}$. Since $x_1 = x_0 + 3\,u = 2 + 3\,u$, we get

$$2 \cdot (2 + 3\,u) \equiv 1 \pmod{3^2},$$

so $u = 1$ and $x_1 = 2 + 1 \cdot 3 = 5$. Proceeding in this manner,

$$x = 2 + 1 \cdot 3 + 1 \cdot 3^2 + \cdots$$

That is, $x_0 = 2$, $x_1 = 2 + 1 \cdot 3 = 5$, $x_2 = 2 + 1 \cdot 3 + 1 \cdot 3^2 = 14$, and so on. We have indeed

$$2\,x = 2 + 2\,(\underbrace{1 + 3 + 3^2 + \cdots}_{-1/2}) = 2 - 1 = 1.$$

Where we compute the infinite sum using the "geometric progression formula"

$$1 + 3 + 3^2 + \cdots = \frac{1}{1-3} = -\frac{1}{2}$$

(formulas as $\sum\limits_{0 \le k} x^k = \frac{1}{1-x}$ make sense for p-adic numbers when $p \mid x$; more precisely, when $|x|_p < 1$—see below the discussion of absolute values and convergence). ▲

In general, $\mathbb{Z}_p$ contains the set of "p-integral numbers"

$$\mathbb{Q} \cap \mathbb{Z}_p = \{\frac{a}{b} \mid a, b \in \mathbb{Z},\ p \nmid b\}.$$

Theorem 1.11. *Every number $\alpha \in \mathbb{Z}_p$, $\alpha \neq 0$, can be uniquely represented as $p^n \epsilon$ where $n = 0, 1, 2, \ldots$ and $\epsilon \in \mathbb{Z}_p^\times$.*

Proof of the theorem. Look at the p-adic expansion of α:

$$\alpha = a_0 + a_1\,p + a_2\,p^2 + \cdots$$

Let n be the smallest index i such that $a_i \neq 0$. Then we have

$$\alpha = a_n\,p^n + a_{n+1}\,p^{n+1} + a_{n+2}\,p^{n+2} + \cdots = p^n\,(a_n + a_{n+1}\,p + a_{n+2}\,p^2 + \cdots).$$

The number $\epsilon := a_n + a_{n+1}\,p + a_{n+2}\,p^2 + \cdots$ is a unit since $a_n \neq 0$.

Now we need to show that the presentation $p^n\,\epsilon$ is unique. Assume $\alpha = p^n\,\epsilon = p^s\,\eta$ for some integers n and s and some units ϵ and η.

$$p^n\,\underbrace{(a_n + a_{n+1}\,p + a_{n+2}\,p^2 + \cdots)}_{\epsilon} = p^s\,\underbrace{(a'_s + a'_{s+1}\,p + a'_{s+2}\,p^2 + \cdots)}_{\eta}.$$

By uniqueness of p-adic expansions, we should have $n = s$ and $a_i = a'_i$ for all i. ■

Corollary 1.12. *$\mathbb{Z}_p$ is an integral domain, i.e. for $\alpha, \beta \in \mathbb{Z}_p$ if $\alpha\,\beta = 0$ then $\alpha = 0$ or $\beta = 0$.*

Proof. Assume $\alpha \neq 0$ and $\beta \neq 0$. We have $\alpha = p^m\,\epsilon$, $\beta = p^s\,\eta$, and $\alpha\,\beta = p^{m+s}\,\epsilon\,\eta = p^{m+s}\,\theta$ for some unit $\theta := \epsilon\,\eta$.

$$\alpha\,\beta = p^{m+s}\,\underbrace{(a_{m+s} + a_{m+s+1}\,p + a_{m+s+2}\,p^2 + \cdots)}_{\theta}.$$

We have $a_{m+s} \neq 0$ and so $\alpha\,\beta \neq 0$. ■

If $\alpha = p^n\,\epsilon$ is the representation of a p-adic number as above, then we define the **p-adic order** of α to be $\nu_p(\alpha) := n$. We also put $\nu_p(0) := \infty$. It satisfies the following properties:

- $\nu_p(\alpha) = \infty$ iff $\alpha = 0$.
- $\nu_p(\alpha\,\beta) = \nu_p(\alpha) + \nu_p(\beta)$.

- $\nu_p(\alpha+\beta) \geq \min\{\nu_p(\alpha), \nu_p(\beta)\}$, with equality when $\nu_p(\alpha) \neq \nu_p(\beta)$.

Indeed, let $\alpha = p^n \epsilon$ and $\beta = p^s \eta$. Suppose $n > s$. Then

$$\alpha + \beta = p^s (p^{n-s} \epsilon + \eta).$$

We claim that $p^{n-s}\epsilon + \eta$ is a unit. Indeed, $p^{n-s}\epsilon \equiv 0 \pmod{p}$ and $\eta \not\equiv 0 \pmod{p}$, so $p^{n-s}\epsilon + \eta \not\equiv 0 \pmod{p}$. So $\nu_p(\alpha+\beta) = s = \min\{\nu_p(\alpha), \nu_p(\beta)\}$.

For $n = s$ in general we have only $\nu_p(\alpha+\beta) \geq s$—it can be the case that $\epsilon + \eta$ is not a unit.

Proposition 1.13. *Let $\alpha, \beta \in \mathbb{Z}_p$. Then $\alpha \mid \beta$ in $\mathbb{Z}_p$ iff $\nu_p(\alpha) \leq \nu_p(\beta)$.*

Proof. If $\alpha \mid \beta$ then $\beta = \alpha\gamma$, so $\nu_p(\beta) = \nu_p(\alpha) + \nu_p(\gamma) \geq \nu_p(\alpha)$.

In the other direction, if $\nu_p(\alpha) \leq \nu_p(\beta)$, then we have $\alpha = p^n \epsilon$ and $\beta = p^s \eta$ with $s \geq n$.

$$\beta = p^n \epsilon \underbrace{p^{s-n} \eta \epsilon^{-1}}_{=:\gamma} = \alpha\gamma.$$

■

Recall that if R is an integral domain, then we say that an element $\alpha \neq 0$ is **irreducible** if $\alpha \notin R^\times$ and $\alpha = \beta\gamma$ implies $\beta \in R^\times$ or $\gamma \in R^\times$. That is, α is not a product of two non-units. We see that the only irreducible element in $\mathbb{Z}_p$ is p (up to multiplication by a unit).

Proposition 1.14. *The only maximal ideal in $\mathbb{Z}_p$ is $p\mathbb{Z}_p$, and all ideals in $\mathbb{Z}_p$ are powers of the maximal ideal.*

Proof. Let I be an ideal in $\mathbb{Z}_p$. Consider $n := \min\{\nu_p(\alpha) \mid \alpha \in I\}$. We claim that $I = p^n\mathbb{Z}_p$.

There exists $\alpha \in I$ such that $\nu_p(\alpha) = n$, namely $\alpha = p^n\epsilon$ for some $\epsilon \in \mathbb{Z}_p^\times$. Now $p^n = \alpha\epsilon^{-1} \in I$, thus $I \supseteq p^n\mathbb{Z}_p$.

If $\beta \in I$, then $\beta = p^s\eta$, with $s = \nu_p(\beta) \geq n$. So $\beta = p^n\gamma$ with $\gamma = p^{n-s}\eta$ and $\beta \in p^n\mathbb{Z}_p$. Hence $I \subseteq p^n\mathbb{Z}_p$.

In particular, the only maximal ideal is $p\mathbb{Z}_p$. ■

This means that $\mathbb{Z}_p$ is a **discrete valuation ring**. Knowing that all ideals in $\mathbb{Z}_p$ have form (p^n), it is natural to ask what are the quotient rings $\mathbb{Z}_p/(p^n)$.

First we see that there is a surjective map

$$\begin{aligned} \mathbb{Z} &\hookrightarrow \mathbb{Z}_p \twoheadrightarrow \mathbb{Z}_p/(p^n), \\ x &\longmapsto (x, x, \ldots) \longmapsto (x, x, \ldots) \bmod p^n \end{aligned}$$

Here we take an integer x and then look at it as a p-adic number (represented by a sequence $(x, x, x, \ldots)$), modulo p^n. The surjectivity is clear: any p-adic number

$$\alpha = a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1} + a_n p^n + \cdots$$

modulo p^n is equivalent to $a_0 + a_1 p + \cdots + a_{n-1} p^{n-1}$, which is an ordinary integer. On the other hand, it is clear that the map sends x to $0 \in \mathbb{Z}_p/(p^n)$ iff x is divisible by p^n. Thus the kernel is $p^n\mathbb{Z}$, and

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

2 Field of p-adic numbers $\mathbb{Q}_p$

Definition 2.1. The field of **p-adic numbers** $\mathbb{Q}_p$ is the fraction field of $\mathbb{Z}_p$.

Proposition 2.2. *Every $\alpha \in \mathbb{Q}_p^\times$ is represented in a unique way as $p^n \epsilon$ where $n \in \mathbb{Z}$ and $\epsilon \in \mathbb{Z}_p^\times$ is a p-adic unit.*

Proof. We have $\alpha = \frac{p^r \epsilon}{p^s \zeta}$ for some units $\epsilon, \zeta \in \mathbb{Z}_p^\times$ and so $\alpha = p^{r-s}\theta$, where $\theta := \epsilon\zeta^{-1}$.

For the uniqueness assume $\alpha = p^n\theta = p^s\eta$. Take r big enough such that $r+n$ and $r+s$ are both nonnegative. Then

$$p^r\alpha = p^{r+n}\theta = p^{r+s}\eta \in \mathbb{Z}_p.$$

By uniqueness of the corresponding representation for the p-adic integers, we conclude $n = s$ and $\theta = \eta$. ■

The p-adic order $\nu_p(\cdot)$ extends to $\mathbb{Q}_p$, and we have a map $\nu_p \colon \mathbb{Q}_p \to \mathbb{Z} \cup \{\infty\}$. It satisfies the following properties:

1. $\nu_p(\alpha) = \infty$ iff $\alpha = 0$.
2. $\nu_p(\alpha\beta) = \nu_p(\alpha) + \nu_p(\beta)$.
3. $\nu_p(\alpha+\beta) \geq \min\{\nu_p(\alpha), \nu_p(\beta)\}$, with equality if $\nu_p(\alpha) \neq \nu_p(\beta)$.

This means that we have a **discrete valuation** on $\mathbb{Q}_p$. With respect to this valuation,

$$\mathbb{Z}_p = \{\alpha \in \mathbb{Q}_p \mid \nu_p(\alpha) \geq 0\}.$$

3 Topology and convergence on $\mathbb{Q}_p$

Intuitively, a p-adic number $\alpha \in \mathbb{Q}_p$ is "small" if it is divisible by a high power of p. That is, if $\nu_p(\alpha)$ is large. So to define the **p-adic absolute value** on $\mathbb{Q}_p$, we pick $\rho \in (0,1)$ and put $|\alpha|_p := \rho^{\nu_p(\alpha)}$. This satisfies the following properties:

- $|\alpha|_p = 0$ iff $\alpha = 0$.
- $|\alpha\beta|_p = |\alpha|_p \cdot |\beta|_p$.
- $|\alpha+\beta|_p \leq \max\{|\alpha|_p, |\beta|_p\}$ with equality if $|\alpha|_p \neq |\beta|_p$.

This defines a **metric** on $\mathbb{Q}_p$ with distance $d(\alpha,\beta) := |\alpha-\beta|_p$. That is, the following properties are satisfied:

- $d(\alpha,\beta) = d(\beta,\alpha)$.
- $d(\alpha,\beta) = 0$ iff $\alpha = \beta$.
- $d(\alpha,\gamma) \leq d(\alpha,\beta) + d(\beta,\gamma)$.

Actually, instead of the triangle inequality, a stronger **ultrametric inequality** $d(\alpha,\gamma) \leq \max\{d(\alpha,\beta), d(\beta,\gamma)\}$ holds.

With respect to this metric, the subspace $\mathbb{Z}_p$ of p-adic integers is the unit ball centered in 0:

$$\mathbb{Z}_p = \{\alpha \in \mathbb{Q}_p \mid |\alpha|_p \leq 1\}.$$

Note that the choice of $\rho \in (0,1)$ above does not affect the topological properties of $\mathbb{Q}_p$; for arithmetical reasons, later on we will fix $\rho = 1/p$ (see p. 12).

Definition 3.1. A sequence of p-adic numbers (α_n) is said to **converge** to $\alpha \in \mathbb{Q}_p$ if

$$\lim_{\substack{\leftarrow \\ n\to\infty}} \nu_p(\alpha_n - \alpha) = \infty;$$

equivalently,

$$\lim_{\substack{\leftarrow \\ n\to\infty}} |\alpha_n - \alpha|_p = 0.$$

This is the same as convergence in the metric space $(\mathbb{Q}_p, d)$.

Example 3.2. The sequence $p, p^2, p^3, \ldots$ converges to 0 in $\mathbb{Q}_p$ since $\nu_p(p^n) = n$ tends to ∞. ▲

Example 3.3. Let $\alpha \in \mathbb{Z}_p$ be a p-adic integer represented by a sequence $(x_0, x_1, x_2, \ldots)$ with $x_n \equiv x_{n-1} \pmod{p^n}$. So $x_n - x_{n-1} \equiv 0 \pmod{p^n}$, meaning $\nu_p(x_n - x_{n-1}) \geq n$. Thus the sequence $(x_n - x_{n-1})$ converges to 0 in $\mathbb{Z}_p$. ▲

Example 3.4. Let $\alpha \in \mathbb{Z}_p$ be a p-adic integer represented by a sequence $(x_0, x_1, x_2, \ldots)$ with $x_n \equiv x_{n-1} \pmod{p^n}$. Consider a sequence of p-adic numbers $(\alpha - x_n)$. One has $\nu_p(\alpha - x_n) \geq n+1$, which tends to ∞ as $n \to \infty$. This is clear if we look at p-adic expansions:

$$\begin{aligned} x_0 &= a_0, \\ x_1 &= a_0 + a_1\, p, \\ x_2 &= a_0 + a_1\, p + a_2\, p^2, \\ &\cdots \\ \alpha &= a_0 + a_1\, p + a_2\, p^2 + \cdots \end{aligned}$$

So if $\alpha \in \mathbb{Z}_p$ is represented by a sequence $(x_0, x_1, x_2, \ldots)$, then this sequence converges to α.

This also gives a precise sense to p-adic expansions $\alpha = "\sum_{n\geq 0} a_n\, p^n"$ that were introduced as formal expressions: the sum on the right hand side indeed converges to α, treated as a limit of partial sums $x_n = (\sum_{0\leq i\leq n} a_i\, p^i)_n$. ▲

From this example we see that each α is a limit of a sequence of integers. Thus $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, and similarly $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. Now we investigate other topological properties of $\mathbb{Q}_p$, and $\mathbb{Z}_p$ as its subspace.

Theorem 3.5. *$\mathbb{Z}_p$ is **sequentially compact**. That is, every infinite sequence in $\mathbb{Z}_p$ contains a convergent subsequence.*

Proof. Let (α_n) be an infinite sequence in $\mathbb{Z}_p$ with terms

$$\alpha_n = a_{n,0} + a_{n,1}\, p + a_{n,2}\, p^2 + \cdots$$

There exists an infinite number of n such that the 0-th p-adic digit of α_n is some $a_{n,0} = a_0$. We take the subsequence $(\alpha_n^{(0)})$ of such numbers. Similarly, there should be a subsequence $(\alpha_n^{(1)})$ with 1-st p-adic digit being equal to some a_1, and so on. So there is a chain of such subsequences $(\alpha_n^{(0)}), (\alpha_n^{(1)}), (\alpha_n^{(2)}), \ldots$. One can take the "diagonal sequence" (β_k) with $\beta_k := \alpha_k^{(k)}$, which is a subsequence of (α_n) by construction. Also by construction, it converges to the p-adic number

$$\beta = a_0 + a_1\, p + a_2\, p^2 + \cdots$$

■

Corollary 3.6. *$\mathbb{Q}_p$ is **locally compact**. That is, every bounded sequence in $\mathbb{Q}_p$ has a convergent subsequence.*

Proof. Let (α_n) be a bounded sequence in $\mathbb{Q}_p$. This means that $|\alpha_n|_p = \rho^{\nu_p(\alpha_n)} \leq A$ for some $A \in \mathbb{R}_{\geq 0}$.

Take some s big enough such that $|p^s|_p \leq \frac{1}{A}$. Consider the sequence $(p^s\, \alpha_n)_n$. Then $|p^s\, \alpha_n|_p = |p^s|_p \cdot |\alpha_n|_p \leq \frac{1}{A}\, A = 1$, thus $p^s\, \alpha_n \in \mathbb{Z}_p$. By the previous theorem, the sequence $(\beta_n) = (p^s\, \alpha_n)_n$ has a convergent subsequence $(\beta_{n_k})_k$. That is, there is some $\beta \in \mathbb{Z}_p$ such that $\nu_p(\beta - \beta_{n_k}) \to \infty$ as $k \to \infty$. The sequence $(\alpha_{n_k})_k$ is a subsequence of $(\alpha_n)_n$, and it converges to the p-adic number β/p^s since $\nu_p(\beta/p^s - \alpha_{n_k}) = \nu_p(\beta/p^s - \beta_{n_k}/p^s) = \nu_p(1/p^s \cdot (\beta - \beta_{n_k})) = \nu_p(1/p^s) + \nu_p(\beta - \beta_{n_k})$, which tends to ∞ as $k \to \infty$. ■

Theorem 3.7. *A sequence (α_n) in $\mathbb{Q}_p$ converges iff $(\alpha_n - \alpha_{n-1})_n$ converges to zero.*

Proof. Assume (α_n) converges to some $\alpha \in \mathbb{Q}_p$. Then $|\alpha_n - \alpha|_p \to 0$. That is, for each $\epsilon > 0$ there exists N such that $|\alpha_n - \alpha|_p \leq \epsilon$ for all $n \geq N$. But now

$$|\alpha_{n+1} - \alpha_n|_p = |(\alpha_{n+1} - \alpha) + (\alpha - \alpha_n)|_p \leq \max\{|\alpha_{n+1} - \alpha|_p, |\alpha - \alpha_n|_p\} \leq \epsilon,$$

so $\alpha_n - \alpha_{n-1} \to 0$.

Assume now that $(\alpha_n - \alpha_{n-1})_n$ converges to zero. This means that the sequence $(\alpha_n - \alpha_{n-1})_n$ is bounded. We can choose A such that $|\alpha_0|_p \leq A$ and $|\alpha_n - \alpha_{n-1}|_p \leq A$ for all $n \geq 1$. So this means

$$\begin{aligned} |\alpha_n|_p &= |\alpha_n - \alpha_{n-1} + \alpha_{n-1} - \alpha_{n-1} + \cdots + \alpha_1 - \alpha_0 + \alpha_0|_p \\ &= |(\alpha_n - \alpha_{n-1}) + (\alpha_{n-1} - \alpha_{n-1}) + \cdots + (\alpha_1 - \alpha_0) + \alpha_0|_p \\ &\leq \max(|\alpha_n - \alpha_{n-1}|_p, \ldots, |\alpha_1 - \alpha_0|_p, |\alpha_0|_p) \leq A, \end{aligned}$$

and (α_n) is a bounded sequence in $\mathbb{Q}_p$. It has a subsequence $(\alpha_{n_k})_k$ converging to some α, because $\mathbb{Q}_p$ is locally compact. So for each $\epsilon > 0$ there exists K such that $|\alpha - \alpha_k|_p < \epsilon$ for all $k \geq K$. But $\alpha_n - \alpha_{n-1}$ converges to zero, so there exists N such that $|\alpha_n - \alpha_{n-1}|_p < \epsilon$ for all $n \geq N$. Thus for $n \geq N$ and $n \geq n_K$ we have

$$\begin{aligned} |\alpha_n - \alpha|_p &= |\alpha_n - \alpha_{n-1} + \alpha_{n-1} + \cdots + \alpha_{n_K+1} - \alpha_{n_K} + \alpha_{n_K} - \alpha|_p \\ &\leq \max\{|\alpha_n - \alpha_{n-1}|_p, \ldots, |\alpha_{n_K+1} - \alpha_{n_K}|_p, |\alpha_{n_K} - \alpha|_p\} < \epsilon. \end{aligned}$$

So $|\alpha_n - \alpha|_p < \epsilon$ for n big enough, and (α_n) converges to α. ■

Remark 3.8. The last theorem actually means that $\mathbb{Q}_p$ is a **complete metric space**, that is, a sequence converges in $\mathbb{Q}_p$ iff it is **Cauchy**, meaning that for each $\epsilon > 0$ there exists N such that $|\alpha_n - \alpha_m| < \epsilon$ for all $n, m \geq N$.

The Cauchy condition of course always implies that $\alpha_n - \alpha_{n-1} \to 0$, but actually for $\mathbb{Q}_p$ the latter is *equivalent* to the Cauchy condition, since

$$|\alpha_n - \alpha_m|_p = |\alpha_n - \alpha_{n-1} + \alpha_{n-1} - \alpha_{n-2} + \cdots + \alpha_{m+1} - \alpha_m|_p \leq \max\{|\alpha_n - \alpha_{n-1}|_p, \ldots, |\alpha_{m+1} - \alpha_m|_p\}.$$

Note that this depends strongly on the ultrametric inequality $|x + y|_p \leq \max\{|x|_p, |y|_p\}$, and in the proof of the theorem above we use the same trick.

The last theorem is *not* true for all complete metric spaces. For example, in $\mathbb{R}$ with the usual Euclidean metric the sequence $(\sum_{1 \leq i \leq n} \frac{1}{i})_n$ satisfies the condition from the theorem, but it is not Cauchy, and indeed the harmonic series $\sum_{n \geq 1} \frac{1}{n}$ diverges.

Corollary 3.9. *The series $\sum_{n \geq 0} \alpha_n$ converges in $\mathbb{Q}_p$ iff the sequence (α_n) converges to zero.*

Proof. The series is by definition given by the sequence $(\sum_{0 \leq i \leq n} \alpha_i)_n$, so it converges iff $(\sum_{0 \leq i \leq n} \alpha_i - \sum_{0 \leq i \leq n-1} \alpha_i)_n = (\alpha_n)_n$ converges to zero. ■

4 Fields with absolute values

Definition 4.1. Let K be a field. An **absolute value** is a function $|\cdot| \colon K \to \mathbb{R}_{\geq 0}$ satisfying the following properties:

1. $|\alpha| = 0$ iff $\alpha = 0$.
2. Multiplicativity: $|\alpha\beta| = |\alpha| \cdot |\beta|$ for all $\alpha, \beta \in K$.
3. Triangle inequality: $|\alpha + \beta| \leq |\alpha| + |\beta|$ for all $\alpha, \beta \in K$.

In particular, multiplicativity implies that $|1| = 1$.

Example 4.2.
- The usual absolute values on $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ give examples of absolute values in the sense of the definition above.
- The p-adic absolute value $|\cdot|_p$ on $\mathbb{Q}_p$ is an absolute value. It is also an absolute value on the subfield $\mathbb{Q} \subset \mathbb{Q}_p$.
- There is always the trivial absolute value given by $|\alpha| := 1$ for all $\alpha \neq 0$.
- If $K = F(t)$ where F is another field, then for $x \in F(t)$ the **order of vanishing** at $\alpha \in F$ is given by $\operatorname{ord}_\alpha x := m$ such that $(t-\alpha)^{-m}$ has no zeroes and no poles at α.

  So $\operatorname{ord}_\alpha x > 0$ if x has a zero at α and $\operatorname{ord}_\alpha x < 0$ if x has a pole at α.

  $|\cdot|_\alpha := \operatorname{ord}_\alpha(\cdot)$ is an absolute value on $F(t)$.

▲

A field K with an absolute value $|\cdot|$ is a metric space with respect to the distance $d(\alpha, \beta) := |\alpha - \beta|$. We call K a **complete field** if it is complete as a metric space (i.e. every Cauchy sequence converges).

Example 4.3.
- $\mathbb{Q}$ is not complete. The completion of $\mathbb{Q}$ with respect to the usual absolute value $|\cdot|$ is $\mathbb{R}$. The completion of $\mathbb{Q}$ with respect to a p-adic absolute value $|\cdot|_p$ is $\mathbb{Q}_p$.
- For $\mathbb{R}$ we can take $\mathbb{C}$, its algebraic closure. It is again complete with respect to the usual absolute value on $\mathbb{C}$.
- $\mathbb{Q}_p$ is not algebraically closed. If we take the algebraic closure $(\mathbb{Q}_p)^{\mathrm{alg}}$, then is not complete, but its completion is algebraically closed; it is usually denoted by $\mathbb{C}_p$.
- The completion of $F(t)$ with respect to $|\cdot|_0 := \operatorname{ord}_0(\cdot)$ is the field of Laurent series $F((t))$.

▲

For every field K we can consider the subring $\mathbb{Z}_K$ generated by 1 (the smallest subring). It is isomorphic either to $\mathbb{Z}$ if $\operatorname{char} K = 0$ or to $\mathbb{F}_p$ if $\operatorname{char} K = p > 0$.

Definition 4.4. We say that the absolute value $|\cdot|$ on K is **archimedian** if it is not bounded on $\mathbb{Z}_K$, and **nonarchimedian** otherwise.

Trivially, a field of characteristic $p > 0$ has only nonarchimedian absolute values.

Observe that a nonarchimedian absolute value should satisfy $|x| \leq 1$ for all $x \in \mathbb{Z}_K$, otherwise the absolute value of $|x^n|$ is not bounded.

Example 4.5. The usual absolute value is archimedian.

The p-adic absolute value $|\cdot|_p$, the trivial absolute value, the absolute value $|\cdot|_\alpha$ on $F(t)$ are all nonarchimedian.

▲

Theorem 4.6. *Let K be a field with an absolute value $|\cdot|$. The following are equivalent:*

1. *$|\cdot|$ is nonarchimedian.*
2. *$|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\}$.*

Proof. Clearly (2) implies (1): for $n = 1 + 1 + \cdots + 1 \in \mathbb{Z}_K$ one has

$$|n| \leq \max\{|1|, |1|, \ldots, |1|\} = 1.$$

In the other direction (1) $\Rightarrow$ (2) — an exercise. ■

Remark 4.7. For a nonarchimedian absolute value $|\cdot|$ one has

$$|\alpha+\beta| = \max\{|\alpha|,|\beta|\} \quad \text{for} \quad |\alpha| \neq |\beta|.$$

Indeed, assume $|\alpha| > |\beta|$. Then $|\alpha+\beta| \leq |\alpha|$, but also $|\alpha| = |(\alpha+\beta)-\beta| \leq \max\{|\alpha+\beta|,|\beta|\} = |\alpha+\beta|$. Thus $|\alpha+\beta| = |\alpha|$.

Definition 4.8. Let $|\cdot|_1$ and $|\cdot|_2$ be absolute values on K. Then we say that they are **equivalent**, $|\cdot|_1 \sim |\cdot|_2$, if they define the same topology on K (that is, every sequence (α_n) converges to α with respect to $|\cdot|_1$ iff it converges to α with respect to $|\cdot|_2$).

Example 4.9. Consider the absolute value $|\cdot|_{1/2}$ on $\mathbb{R}$ or $\mathbb{Q}$ given by $|\alpha|_{1/2} := |\alpha|^{1/2}$. It is equivalent to the usual absolute value.

Define a p-adic absolute value on $\mathbb{Q}$ by $|\cdot|_p := \rho^{\nu_p(\alpha)}$ for $\rho \in (0,1)$. Different choices of ρ lead to different but equivalent absolute values. ▲

In general, if $|\cdot|$ is an absolute value, then $|\cdot|^\lambda$ is an absolute value equivalent to $|\cdot|$, if holds

- $\lambda \in (0,1]$ when $|\cdot|$ is archimedian,
- $\lambda \in (0,+\infty)$ when $|\cdot|$ is nonarchimedian.

Theorem 4.10. *Let $|\cdot|_1$ and $|\cdot|_2$ be absolute values on K. The following are equivalent:*

1. $|\cdot|_1 \sim |\cdot|_2$.
2. *There exists $\lambda \in \mathbb{R}_{\geq 0}$ such that $|\cdot|_2 = |\cdot|_1^\lambda$.*

Proof. (2) ⇒ (1) is clear, (1) ⇒ (2) is an exercise. ■

Theorem 4.11 (Weak approximation theorem)**.** *Let K be a field. Let $|\cdot|_1,\ldots,|\cdot|_m$ be pairwise nonequivalent absolute values (finitely many). Let $\alpha_1,\ldots,\alpha_m \in K$ and let $\epsilon > 0$. Then there exists $\alpha \in K$ such that*

$$|\alpha-\alpha_1|_1,\ldots,|\alpha-\alpha_m|_m < \epsilon.$$

Proof is left as an exercise (rather tricky).

Example 4.12. Let $K = \mathbb{Q}$ and let $p_1,\ldots,p_m$ be distinct primes and $s_1,\ldots,s_m$ be natural numbers. For $\alpha_1,\ldots,\alpha_m \in \mathbb{Z}$ there exists $\alpha \in \mathbb{Z}$ such that

$$\begin{aligned} \alpha &\equiv \alpha_1 \pmod{p_1^{s_1}},\\ &\cdots\\ \alpha &\equiv \alpha_m \pmod{p_m^{s_m}}. \end{aligned}$$

So the weak approximation theorem generalizes the Chinese remainder theorem. ▲

Let K_i be the completions of K with respect to the absolute values $|\cdot|_i$. We may consider the diagonal embedding

$$\begin{aligned} K &\hookrightarrow K_1 \times \cdots \times K_m,\\ \alpha &\mapsto (\alpha,\ldots,\alpha). \end{aligned}$$

The weak approximation theorem is equivalent to saying that the image of this map is dense.

We know the following examples of absolute values on $\mathbb{Q}$: the usual $|\cdot|$, the p-adic $|\cdot|_p$ for each prime p, and the trivial one. In fact, that is all.

Theorem 4.13 (Ostrowski)**.** *Every nontrivial absolute value on $\mathbb{Q}$ is equivalent either to $|\cdot|$, or to $|\cdot|_p$ for some p.*

Proof is left as an exercise (easy for nonarchimedian absolute values; a bit harder to show that there is only the usual archimedian absolute value).

We denote by $M_{\mathbb{Q}}$ the set of all absolute values on $\mathbb{Q}$ up to equivalence. We want to pick convenient representatives in every equivalence class:

- $|\cdot|$ is the usual archimedian absolute value.
- For every prime p take $|\alpha|_p := \rho^{v_p(\alpha)}$ with $\rho = 1/p$. That is, $|\alpha|_p := p^{-v_p(\alpha)}$.

Now by $M_{\mathbb{Q}} = \{2,3,5,7,11,\ldots\} \cup \{\infty\}$ we denote the set of "normalized" absolute values. We treat $|\cdot|$ as an absolute value $|\cdot|_\infty$ coming from an "infinite prime".

Theorem 4.14 (Product formula)**.** *Let $\alpha \in \mathbb{Q}^\times$. Then*

$$\prod_{p \in M_{\mathbb{Q}}} |\alpha|_p = 1.$$

Proof. Consider a function $\phi(\alpha) := \prod_{p \in M_{\mathbb{Q}}} |\alpha|_p$. It is multiplicative, so it is enough to verify the statement for the generators of $\mathbb{Q}^\times$, that is for prime numbers.

$$|q|_p = \begin{cases} q^{-1}, & p = q, \\ q, & p = \infty, \\ 1, & \text{otherwise.} \end{cases}$$

$$\prod_{p \in M_{\mathbb{Q}}} |q|_p = q^{-1}\, q = 1.$$

■

Example 4.15. Let $\alpha = -12/5$. Then we have

$$|\alpha|_2 = \frac{1}{4},\ |\alpha|_3 = \frac{1}{3},\ |\alpha|_5 = 5,\ |\alpha|_\infty = \frac{12}{5},$$

$$|\alpha|_p = 1 \quad \text{for } p \neq 2,3,5.$$

And so indeed

$$\prod_{p \in M_{\mathbb{Q}}} |\alpha|_p = \frac{1}{4} \cdot \frac{1}{3} \cdot 5 \cdot \frac{12}{5} = 1.$$

▲

The product formula can be generalized to any number field $K/\mathbb{Q}$—see p. 61.

5 Equations over p-adic numbers

We relate equations over p-adic numbers to congruences modulo p^k.

Theorem 5.1. *Let $F(X_1,\ldots,X_n) \in \mathbb{Z}[X_1,\ldots,X_n]$ be a polynomial with integer coefficients. Let p be a prime number. The following are equivalent:*

1. *For all $k = 1,2,3,\ldots$ the congruence $F(X_1,\ldots,X_n) \equiv 0 \pmod{p^k}$ has a solution.*
2. *The equation $F(X_1,\ldots,X_n) = 0$ has a solution in $\mathbb{Z}_p$.*

Proof. Suppose $\underline{\alpha} = (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}_p^n$ is a solution of an equation $F(\underline{X}) = 0$. Then looking at the identity $F(\underline{\alpha}) = 0$ modulo p^k, we have a congruence $F(\underline{a}) \equiv 0 \pmod{p^k}$ with some $\underline{a} \in \mathbb{Z}^n$ (recall that $\mathbb{Z}_p/(p^k) \cong \mathbb{Z}/p^k\mathbb{Z}$).

Now suppose that for $k = 1, 2, 3, \dots$ there exists a sequence of integers $\underline{a}^{(k)} = (a_1^{(k)}, \dots, a_n^{(k)})$ such that $F(\underline{a}^{(k)}) \equiv 0 \pmod{p^k}$. Since $\mathbb{Z}_p$ is sequentially compact, we may assume that this sequence is convergent to some $\underline{\alpha} \in \mathbb{Z}_p^n$ (by replacing it with some subsequence). Now $F(\underline{\alpha}) = \varprojlim_{k\to\infty} F(\underline{a}^{(k)}) = 0$, because $|F(\underline{a}^{(k)})| \le p^{-k}$. ■

Moreover, if F is, say, a quadratic form, then *nontrivial* solutions of $F(\underline{X}) = 0$ correspond to *nontrivial* solutions of $F(\underline{X}) \equiv 0 \pmod{p^k}$. Now we can restate our goal, the Hasse–Minkowski theorem (1.2), in the following way:

Theorem 5.2 (Local–global principle; Hasse, Minkowski)**.** *Let $F(X_1, \dots, X_n) \in \mathbb{Z}[X_1, \dots, X_n]$ be a quadratic form. The following conditions are equivalent:*

1. *Local: $F(\underline{X}) = 0$ has a nontrivial solution in $\mathbb{Q}_p^n$ for each $2 \le p \le \infty$.*
2. *Global: $F(\underline{X}) = 0$ has a nontrivial solution in $\mathbb{Q}^n$.*

6 Hensel's lemma

Here we will prove the Hensel's lemma, a vital tool which will be used in many subsequent proofs.

Theorem 6.1 (Hensel's Lemma, first form)**.** *Let $f(X) \in \mathbb{Z}_p[X]$ be a p-adic polynomial and assume there exists $\alpha_0 \in \mathbb{Z}_p$ such that $f(\alpha_0) \equiv 0 \pmod{p}$ but $f'(\alpha_0) \not\equiv 0 \pmod{p}$. Then there exists a unique $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ and $\alpha \equiv \alpha_0 \pmod{p}$.*

Example 6.2. *There exists $\alpha \in \mathbb{Z}_7$ such that $\alpha^2 \equiv 2 \pmod 7$ and $\alpha \equiv 3 \pmod 7$.*

For this apply the Hensel's lemma to $f(X) = X^2 - 2$ and $\alpha_0 = 3$. We have $f(\alpha_0) = 7 \equiv 0 \pmod 7$ and $f'(\alpha_0) = 6 \not\equiv 0 \pmod 7$.

This is the 7-adic square root of 2:

$$\sqrt{2} = 3 + 7 + 2\cdot 7^2 + 6\cdot 7^3 + 7^4 + 2\cdot 7^5 + 7^6 + 2\cdot 7^7 + 4\cdot 7^8 + 6\cdot 7^9 + \cdots$$

We already saw this in example 1.4. ▲

Sometimes the stated Hensel's lemma is not enough and one should use its generalization:

Theorem 6.3 (Hensel's Lemma, strong form)**.** *Let $f(X) \in \mathbb{Z}_p[X]$ be a p-adic polynomial and assume there exists $\alpha_0 \in \mathbb{Z}_p$ such that $f(\alpha_0) \equiv 0 \pmod{p^{2k+1}}$ but $f'(\alpha_0) \not\equiv 0 \pmod{p^{k+1}}$. Then there exists a unique $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ and $\alpha \equiv \alpha_0 \pmod{p^{k+1}}$.*

(Usually $k = 1$ is enough.)

Actually Hensel's lemma is valid for any complete nonarchimedian field. Suppose K is complete with respect to a nonarchimedian absolute value $|\cdot|$. Consider its **ring of integers**

$$O_K := \{x \in K \mid |x| \le 1\}.$$

Theorem 6.4 (General Hensel)**.** *Suppose $f(X) \in O_K[X]$ is a polynomial, and $\alpha_0 \in O_K$ is such that $|f(\alpha_0)| < 1$ and $|f'(\alpha_0)| = 1$. Then there exists a unique $\alpha \in O_K$ such that $f(\alpha) = 0$ and $|\alpha - \alpha_0| < 1$.*

Theorem 6.5 (General Hensel, strong form)**.** *Suppose $f(X) \in O_K[X]$ is a polynomial, and $\alpha_0 \in O_K$ is such that $|f(\alpha_0)| < |f'(\alpha_0)|^2$. Then there exists a unique $\alpha \in O_K$ such that $f(\alpha) = 0$ and $|\alpha - \alpha_0| \le \frac{|f(\alpha_0)|}{|f'(\alpha_0)|}$.*

Remark 6.6. In fact Hensel's lemma is about complete *rings*:
Let R be a ring that is complete with respect to the ideal $\mathfrak{m}$. Suppose $f(X) \in R[X]$ is a polynomial, and $\alpha_0 \in R$ is such that $f(\alpha_0) \equiv 0 \pmod{f'(\alpha_0)^2\,\mathfrak{m}}$. Then there exists $\alpha \in R$ such that $f(\alpha) = 0$ and $\alpha \equiv \alpha_0 \pmod{f'(\alpha_0)\,\mathfrak{m}}$. Further, if α_0 is not a zero divisor in R, then α is unique.

See *Eisenbud, Commutative Algebra with a View Toward Algebraic Geometry, Chapter 7* and *Atiyah, Macdonald, Introduction to Commutative Algebra, Exercises 10.9, 10.10.*

We are interested only in the case $R = O_K$, where K is a complete nonarchimedian field.

Proof of the first statement (theorem 6.1). So we suppose we have a polynomial $f(X) \in \mathbb{Z}_p[X]$ and $\alpha_0 \in \mathbb{Z}_p$ such that $f(\alpha_0) \equiv 0 \pmod p$ and $f'(\alpha_0) \not\equiv 0 \pmod p$. We want to find $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ and $\alpha \equiv \alpha_0 \pmod p$. Moreover, we want to show that such α is unique.

We construct a sequence $(\alpha_n)_{n\geq 0}$ such that $\alpha_n \equiv \alpha_{n-1} \pmod{p^n}$ and $f(\alpha_n) \equiv 0 \pmod{p^{n+1}}$. All terms in our sequence will satisfy $\alpha_n \equiv \alpha_0 \pmod p$. In particular, $f'(\alpha_n) \equiv f'(\alpha_0) \not\equiv 0 \pmod p$.

Assume α_{n-1} is defined and $f(\alpha_{n-1}) \equiv 0 \pmod{p^n}$ and $f'(\alpha_{n-1}) \not\equiv 0 \pmod p$. We need to define α_n of the form $\alpha_{n-1} + p^n\,u$ for some u. Look at the "Taylor expansion" around α_{n-1}:

$$f(\alpha_n) = f(\alpha_{n-1}) + f'(\alpha_{n-1})\,(\alpha_n - \alpha_{n-1}) + (\alpha_n - \alpha_{n-1})^2\,g(\alpha_n, \alpha_{n-1}).$$

Here $g(X, Y) \in \mathbb{Z}_p[X, Y]$ gives the rest of the expansion.

We should have $\alpha_n - \alpha_{n-1} = p^n\,u$ for some u, so

$$f(\alpha_n) = f(\alpha_{n-1}) + p^n\,u\,f'(\alpha_{n-1}) + p^{2n}\,u^2\,g(\alpha_n, \alpha_{n-1}) \equiv f(\alpha_{n-1}) + p^n\,u\,f'(\alpha_{n-1}) \pmod{p^{2n}}.$$

As required, $f(\alpha_n) \equiv f(\alpha_{n-1}) \equiv 0 \pmod p$.

Since $f(\alpha_{n-1}) \equiv 0 \pmod{p^n}$, we have $f(\alpha_{n-1}) = v\,p^n$, and in $\alpha_n = \alpha_{n-1} + p^n\,u$ we can substitute $u := -v/f'(\alpha_{n-1})$, that is take

$$\alpha_n := \alpha_{n-1} - \frac{f(\alpha_{n-1})}{f'(\alpha_{n-1})}. \tag{*}$$

Now $|\alpha_n - \alpha_{n-1}|_p \to 0$ as $n \to \infty$, so our sequence converges to some $\alpha \in \mathbb{Z}_p$. For this α we have $f(\alpha) = \varprojlim_{n\to\infty} f(\alpha_n) = 0$. Since $\alpha_n \equiv \alpha_0 \pmod p$, we have $\alpha \equiv \alpha_0 \pmod p$.

Now we found the requested α, and it remains to show its uniqueness. Assume we have also β such that $f(\alpha) = f(\beta) = 0$ and $\alpha \equiv \beta \equiv \alpha_0 \pmod p$. Since $f'(\alpha_0) \not\equiv 0 \pmod p$, we have $f'(\alpha) \not\equiv 0 \pmod p$. As before, we look at a "Taylor expansion". We have an identity in $\mathbb{Z}_p$

$$\underbrace{f(\beta)}_{=0} = \underbrace{f(\alpha)}_{=0} + f'(\alpha)\,(\beta - \alpha) + (\beta - \alpha)^2\,g(\alpha, \beta).$$

Since $f'(\alpha)$ is a unit, we have

$$\beta - \alpha = -(\beta - \alpha)^2\,g(\alpha, \beta)\,f'(\alpha)^{-1}.$$

We compute p-adic norms of both sides: the term $g(\alpha, \beta)\,f'(\alpha)^{-1}$ gives some norm $|g(\alpha, \beta)\,f'(\alpha)^{-1}|_p \leq 1$, so we have a bound

$$|\beta - \alpha|_p \leq |\beta - \alpha|_p^2.$$

But since $|\beta - \alpha|_p < 1$, this inequality means $|\beta - \alpha|_p = 0$, and so $\beta = \alpha$. ■

Observe that in the proof above we used the formula (*), which is the same as in the Newton's method for finding a root of f in $\mathbb{R}$. So we see that in the nonarchimedian case Newton's method always converges.

Proof of the general Hensel (theorem 6.5). We have a polynomial $f(X) \in O_K[X]$ and $\alpha_0 \in O_K$ is such that $|f(\alpha_0)| < |f'(\alpha_0)|^2$. We look for $\alpha \in O_K$ such that $f(\alpha) = 0$ and $|\alpha - \alpha_0| \le \frac{|f(\alpha_0)|}{|f'(\alpha_0)|}$. We will show that such α exists and we omit the proof of its uniqueness.

Denote

$$\delta := \frac{|f(\alpha_0)|}{|f'(\alpha_0)|^2} < 1.$$

We recursively define a sequence $(\alpha_n)_{n\ge 0}$ such that the following formulas hold:

$$|f(\alpha_n)| \le \delta^{2^n} |f'(\alpha_0)|^2, \tag{1}_n$$

$$|\alpha_n - \alpha_{n-1}| \le \delta^{2^{n-1}} |f'(\alpha_0)|, \tag{2}_n$$

$$|f'(\alpha_n)| = |f'(\alpha_0)|. \tag{3}_n$$

Assume we have α_{n-1}. We define the next term again by the Newton's formula

$$\alpha_n := \alpha_{n-1} - \frac{f(\alpha_{n-1})}{f'(\alpha_{n-1})}.$$

We should show that $(1)_n, (2)_n, (3)_n$ follow from $(1)_{n-1}, (2)_{n-1}, (3)_{n-1}$. With this definition of α_n we deduce

$$|\alpha_n - \alpha_{n-1}| = \frac{|f(\alpha_{n-1})|}{|f'(\alpha_{n-1})|} \le \frac{\delta^{2^{n-1}} |f'(\alpha_0)|^2}{|f'(\alpha_0)|} = \delta^{2^{n-1}} |f'(\alpha_0)|.$$

Next we have

$$f(\alpha_n) = \underbrace{f(\alpha_{n-1}) + (\alpha_n - \alpha_{n-1}) f'(\alpha_{n-1})}_{=0} + (\alpha_n - \alpha_{n-1})^2 g(\alpha_n, \alpha_{n-1}),$$

and this gives an estimate

$$|f(\alpha_n)| \le |\alpha_n - \alpha_{n-1}|^2 \le \delta^{2^n} |f'(\alpha_0)|^2.$$

We have another estimate

$$|\alpha_n - \alpha_{n-1}| \le \delta^{2^{n-1}} |f'(\alpha_0)| < |f'(\alpha_0)|.$$

We apply this to the formula

$$f'(\alpha_n) = f'(\alpha_0) + (\alpha_n - \alpha_0) h(\alpha_n, \alpha_0)$$

and get

$$|f'(\alpha_n) - f'(\alpha_0)| = |\alpha_n - \alpha_0| \cdot |h(\alpha_n, \alpha_0)| < |f'(\alpha_0)|.$$

Now $|f'(\alpha_n)| = |f'(\alpha_0)|$, since otherwise the last bound becomes

$$\max\{|f'(\alpha_n)|, |f'(\alpha_0)|\} = |f'(\alpha_0)| < |f'(\alpha_0)|.$$

■

The Hensel's lemma can be generalized to multivariate polynomials.

Theorem 6.7. *Let $F(X_1, \dots, X_n) \in \mathbb{Z}_p[X_1, \dots, X_n]$ be a polynomial in n variables and let $\underline{\gamma} = (\gamma_1, \dots, \gamma_n) \in \mathbb{Z}_p^n$ be such that $F(\underline{\gamma}) \equiv 0 \pmod{p^{2k+1}}$ and there is some $i = 1, \dots, n$ such that $F'_{X_i}(\underline{\gamma}) \not\equiv 0 \pmod{p^{k+1}}$. Then there exists $\underline{\alpha} \in \mathbb{Z}_p^n$ such that $\underline{\alpha} = \underline{\gamma} \pmod{p^{k+1}}$ and $F(\underline{\alpha}) = 0$.*

This reduces to the usual Hensel's lemma. We may assume $i = 1$. Consider $f(X) := F(X, \gamma_2, \dots, \gamma_n)$ and take $\beta_0 := \gamma_1$. Then $f'(\beta_0) = F'_{X_1}(\underline{\gamma})$ and we can conclude that there exists a unique β such that $\beta \equiv \beta_0 \pmod{p^{k+1}}$ and $f(\beta) = 0$. Take $\underline{\alpha} := (\beta, \gamma_2, \dots, \gamma_n)$, and we are done.

As an application of the Hensel's lemma, we investigate the squares in $\mathbb{Q}_p^\times$.

7 Squares in $\mathbb{Q}_p^\times$

In the group of units $\mathbb{Q}_p^\times$ there is a subgroup, which we denote by $(\mathbb{Q}_p^\times)^2$, formed by squares:

$$(\mathbb{Q}_p^\times)^2 := \{\alpha^2 \mid \alpha \in \mathbb{Q}_p^\times\}.$$

We would like to determine the subgroup index $[\mathbb{Q}_p^\times : (\mathbb{Q}_p^\times)^2]$.

The easiest case is $p = \infty$. The subgroup of squares $(\mathbb{R}^\times)^2$ is the multiplicative group of positive numbers, and $[\mathbb{R}^\times : (\mathbb{R}^\times)^2] = 2$.

Assume that $2 < p < \infty$. Consider a unit $\epsilon \in \mathbb{Z}_p^\times$. When is it a square?

Proposition 7.1. *Assume $p \neq 2$. Then ϵ is a square in $\mathbb{Z}_p$ if $\epsilon \bmod p$ is a square in $\mathbb{F}_p$.*

Proof. We apply Hensel's lemma (6.1) to a polynomial $f(X) = X^2 - \epsilon$. Its derivative is $f'(X) = 2X$. If there exists η_0 such that $\eta_0^2 \equiv \epsilon \pmod p$, then automatically $f'(\eta_0) = 2\eta_0 \not\equiv 0 \pmod p$, and by Hensel there exists $\eta \in \mathbb{Z}_p$ such that $\eta^2 = \epsilon$.
(Note that the derivative is $2X$, so our argument depends on the assumption $p \neq 2$!) ■

We have $\mathbb{Z}_p/(p) \cong \mathbb{F}_p$, and $\mathbb{F}_p^\times$ is a cyclic group of order $p-1$. The subgroup of squares $(\mathbb{F}_p^\times)^2$ has index 2. Now $\epsilon \in \mathbb{Z}_p^\times$ is a square iff the image of ϵ in $\mathbb{F}_p^\times$ is a square. Hence $[\mathbb{Z}_p^\times : (\mathbb{Z}_p^\times)^2] = 2$.
An element $\alpha \in \mathbb{Q}_p^\times$ has form $\alpha = p^m\epsilon$ for $\epsilon \in \mathbb{Z}_p^\times$. It is a square iff m is even and ϵ is a square. Hence $[\mathbb{Q}_p^\times : (\mathbb{Q}_p^\times)^2] = 4$.

The situation becomes most complicated for $p = 2$, because of the well-known principle:

all primes are odd and 2 is the oddest.

Proposition 7.2. *A unit $\epsilon \in \mathbb{Z}_2^\times$ is a square in $\mathbb{Z}_2^\times$ iff $\epsilon \equiv 1 \pmod 8$.*

Proof. Assume $\epsilon \equiv 1 \pmod 8$. Apply the Hensel's lemma (the strong form, theorem 6.3) for $f(X) = X^2 - \epsilon$ and $\eta_0 = 1$. We have $F(\eta_0) \equiv 0 \pmod 8$ and $f'(\eta_0) = 2 \not\equiv 0 \pmod 4$. So there exists η such that $\eta^2 - \epsilon = 0$ and $\eta \equiv \eta_0 \pmod 8$. ■

Now we have $\mathbb{Z}_2/(8) \cong \mathbb{Z}/8\mathbb{Z}$ and $(\mathbb{Z}/8\mathbb{Z})^\times \cong C_2 \times C_2$. So $[\mathbb{Z}_2^\times : (\mathbb{Z}_2^\times)^2] = 4$ and $[\mathbb{Q}_2^\times : (\mathbb{Q}_2^\times)^2] = 8$.

To sum up our calculation,

$$[\mathbb{Q}_p^\times : (\mathbb{Q}_p^\times)^2] = \begin{cases} 2, & p = \infty, \\ 4, & 2 < p < \infty, \\ 8, & p = 2. \end{cases}$$

8 Quadratic forms and quadratic spaces

Now we are going to develop some basic theory of quadratic forms that we will need later.

Let K be a field and let U be a vector space over K. Consider a symmetric bilinear form $\psi\colon U \times U \to K$ (recall that this means that $\psi(u,v) = \psi(v,u)$, and $\psi(-,v), \psi(u,-)\colon U \to K$ are both linear maps).
We can define a quadratic form $\phi(u) := \psi(u,u)$; if $\operatorname{char} K \neq 2$, then this in turn defines ψ, e.g. via the **polarization identity**

$$\psi(u,v) = \frac{1}{4}(\phi(u+v) + \phi(u-v)).$$

Indeed,

$$\begin{aligned}
\psi(u,u) &=: \phi(u),\\
2\psi(u,v) &= \phi(u+v) - \phi(u) - \phi(v),\\
2\psi(u,v) &= \phi(u) + \phi(v) - \phi(u-v),\\
4\psi(u,v) &= \phi(u+v) - \phi(u-v).
\end{aligned}$$

So from now on we impose the restriction $\operatorname{char} K \neq 2$ and we will use $\psi\colon U \times U \to K$ and $\phi\colon U \to K$ interchangeably for a bilinear form and the corresponding quadratic form.

Proposition 8.1. *Assume ψ is not identically zero. Then neither is ϕ identically zero.*

Proof. This is immediate from the polarization identity: if $\psi(u,v) \neq 0$, then either $\phi(u+v) \neq 0$ or $\psi(u-v) \neq 0$. ■

Definition 8.2. A pair (U,ψ) consisting of a K-vector space U and a symmetric bilinear map $\psi\colon U \times U \to K$ is called a **quadratic space**. We say that a quadratic space is **regular** if ψ is nondegenerate; that is, if for each $u \neq 0$ the linear map $v \mapsto \psi(u,v)$ is nonzero.

$$\begin{aligned}
U &\to U^\vee := \operatorname{Hom}(U,K),\\
u &\mapsto (v \mapsto \psi(u,v)).
\end{aligned}$$

We will work with finite dimensional vector spaces. We will also treat both (U,ψ) and (U,ϕ) as the same quadratic space.

Proposition 8.3. *The following are equivalent:*

1. *(U,ψ) is regular.*
2. *If $u_1,\dots,u_n$ is a basis of U, then $\det[\psi(u_i,u_j)] \neq 0$.*

(A proof can be found in any linear algebra textbook.)

We call the number $\delta(\phi) = \delta(\psi) := \det[\psi(u_i,u_j)]$ the **discriminant** of the quadratic form. It is not well-defined since there is no canonical basis for U. We consider it modulo squares, i.e. as an element of $K^\times/(K^\times)^2$.

Example 8.4. Let $\dim U = 2$ and u,v be some basis of U. Define in this basis $\psi\colon U \times U \to K$ as follows:

$$\begin{aligned}
\psi(u,v) &= \psi(v,u) = 1,\\
\psi(u,u) &= \psi(v,v) = 0.
\end{aligned}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

The quadratic space (U,ψ) is regular, but the subspaces $\langle u\rangle$ and $\langle v\rangle$ are not regular, since ψ restricted on them is identically zero. ▲

Definition 8.5. Let (U,ψ) be a quadratic space. For a subspace $V \subseteq U$ the **orthogonal complement** (with respect to ψ) is defined to be

$$V^\perp := \{u \in U \mid \psi(u,v) = 0 \text{ for all } v \in V\}.$$

Proposition 8.6. *If (U,ψ) is regular, then $\dim V + \dim V^\perp = \dim U$.*

Proof. Consider a basis $v_1, \dots, v_m$ of V and define a map

$$\begin{aligned} U &\to V, \\ u &\mapsto (\psi(u, v_1), \dots, \psi(u, v_m)). \end{aligned}$$

Since ψ is regular, this is a surjection. The kernel is $V^\perp$. ∎

It is not always the case that $V \cap V^\perp = \{0\}$, however we always have the following.

Proposition 8.7. *Assume U is regular and V is its subspace. Then $(V^\perp)^\perp = V$.*

Proof. It is clear that $V \subseteq (V^\perp)^\perp$.
On the other hand, we have

$$\begin{aligned} \dim V + \dim V^\perp &= \dim U, \\ \dim V^\perp + \dim (V^\perp)^\perp &= \dim U. \end{aligned}$$

Thus $\dim V = \dim (V^\perp)^\perp$. ∎

Proposition 8.8. *Assume V is a regular subspace of (U, ψ). Then $U = V \oplus V^\perp$.*

(We do not assume that U itself is regular.)

Proof. Take $u \in U$ and consider a map

$$\begin{aligned} f\colon V &\to K, \\ v &\mapsto \psi(u, v). \end{aligned}$$

Since V is regular, there exists $w \in V$ such that $f(v) = \psi(w, v)$ for all $v \in V$.
We have a decomposition $u = w + (u - w)$, and $u - w \in V^\perp$ since $\psi(u - w, v) = \psi(u, v) - \psi(w, v) = 0$ for all $v \in V$. So $U = V + V^\perp$.
Since V is regular, $V \cap V^\perp = \{0\}$, and hence $U = V \oplus V^\perp$. ∎

Proposition 8.9. *Assume U is regular and V is its subspace. The following are equivalent:*

1. *V is regular.*
2. *$V \cap V^\perp = \{0\}$.*
3. *$V^\perp$ is regular.*

Definition 8.10. A basis $u_1, \dots, u_n$ for U is called **orthogonal** (with respect to ψ) if $\psi(u_i, u_j) = 0$ for $i \neq j$.

(N.B. we do not talk about an ortho*normal* basis, just orthogonal.)

Proposition 8.11. *Every quadratic space admits an orthogonal basis.*

Proof. If ψ is identically zero, then any basis will do. If not, there is a vector u_1 such that $\phi(u_1) \neq 0$. Consider a subspace $V := \langle u_1 \rangle$; it is regular, $U = V \oplus V^\perp$, and $\dim V^\perp < \dim U$. By induction on $\dim V^\perp$, the whole U admits an orthogonal basis $u_1, \dots, u_n$. ∎

If (U, ψ) is a regular quadratic space and $u_1, \dots, u_n$ is an orthogonal basis, then $\phi(u_i) \neq 0$.

Isotropy

Definition 8.12. A nonzero vector u such that $\psi(u,u)=0$ is called **isotropic** (with respect to ψ).

We say that a quadratic space (U,ψ) is **isotropic** (or that ψ is isotropic) if there exists an isotropic vector $u\in U$.

Example 8.13. If (U,ψ) is not regular, then it is isotropic. ▲

In example 8.4 we saw isotropic space with ψ given by a matrix $\begin{pmatrix}0&1\\1&0\end{pmatrix}$, that is, in a basis u,v we have $\phi(x\,u+y\,v)=2\,x\,y$. This space is called the **hyperbolic plane** and it plays a special role:

Proposition 8.14. *Let (U,ϕ) be a regular isotropic space. Then $U=V\oplus V^{\perp}$ where V is the hyperbolic plane.*

Proof. Since ψ is isotropic, there exists a nonzero vector $u\in U$ such that $\psi(u,u)=0$. Since ψ is regular, there exists w such that $\psi(u,w)\neq 0$. We may assume $\psi(u,w)=1$. Consider a vector $v=\lambda u+w$ where $\lambda\in K$.

$$\psi(u,v)=\psi(u,\lambda u+w)=\lambda\psi(u,u)+\psi(u,w)=1.$$

Now

$$\psi(v,v)=\psi(\lambda u+w,\lambda u+w)=\lambda^2\underbrace{\psi(u,u)}_{=0}+2\,\lambda\underbrace{\psi(u,w)}_{=1}+\psi(w,w)=2\,\lambda+\psi(w,w).$$

So we take $\lambda=-\frac{1}{2}\psi(w,w)$ and now $\psi(v,v)=0$ (we use our usual assumption $\operatorname{char}K\neq 2$).
Thus $V=\langle u,v\rangle$ is the hyperbolic plane. Since V is regular, $U=V\oplus V^{\perp}$. ■

Definition 8.15. We call a quadratic space (U,ψ) **universal** if for any $\alpha\in K^{\times}$ there exists $u\in U$ such that $\psi(u,u)=\alpha$.

We say in this case that ψ **represents** α.

Example 8.16. For $K=\mathbb{R}$ it is well-known that any quadratic form is equivalent to

$$X_1^2+\cdots+X_r^2-(X_{r+1}^2+\cdots+X_n^2).$$

It is isotropic iff $0<r<n$ and it is also universal iff $0<r<n$. Is it always the case and being universal corresponds to being isotropic? ▲

Proposition 8.17. *Any regular isotropic space is universal.*

Proof. This follows from the fact that the hyperbolic plane is universal. ■

The converse is not true: in general universality does *not* imply isotropy.

Theorem 8.18. *Let K be a finite field with* $\operatorname{char}K\neq 2$. *Then any regular quadratic space over K of dimension ≥ 2 is universal.*

Proof. It is sufficient to consider $\dim U=2$. Let u,v be an orthogonal basis for U. We have

$$\phi(x\,u+y\,v)=x^2\,\phi(u)+y^2\,\phi(v).$$

Here $\phi(u),\phi(v)\neq 0$.
Now if $K=\mathbb{F}_q$, then $K^{\times}$ is a cyclic group of order $q-1$, and the subgroup of squares in $K^{\times}$ has order

$$\#(\mathbb{F}_q^{\times})^2=\frac{q-1}{2}.$$

So there are totally $\frac{q+1}{2}$ squares in $\mathbb{F}_q$, taking into account also 0. We count the number of elements of the form $x^2\,\phi(u)$:

$$\#\{x^2\,\phi(u)\mid x\in\mathbb{F}_q\}=\frac{q+1}{2}.$$

Now for some $\alpha \in \mathbb{F}_q^\times$ count the elements of the form $\alpha - y^2\,\phi(v)$:

$$\#\{\alpha - y^2\,\phi(v) \mid y \in \mathbb{F}_q\} = \frac{q+1}{2}.$$

The number of elements sum up to $q+1$, meaning that the sets are not disjoint. So there exist some $x, y \in \mathbb{F}_q$ such that

$$x^2\,\phi(u) = \alpha - y^2\,\phi(v).$$

Thus for any $\alpha \in \mathbb{F}_q^\times$ we have $\alpha = x^2\,\phi(u) + y^2\,\phi(v) = \phi(x\,y + y\,v)$ for some $x, y \in \mathbb{F}_q$. ■

On the other hand, not every two-dimensional space over a finite field is isotropic. To see it consider $\beta \in \mathbb{F}_q^\times$ which is not a square. Fix an orthogonal basis u, v with $\phi(u) = 1$ and $\phi(v) = -\beta$; that is $\phi(X, Y) = X^2 - \beta\,Y^2$. Then

$$\phi(x\,u + y\,v) = x^2 - \beta\,y^2 \neq 0 \quad \text{for } (x, y) \neq (0, 0).$$

Proposition 8.19. *Let $\phi(X_1, \ldots, X_n)$ be a regular quadratic form over K and $\alpha \in K^\times$. The following are equivalent:*

1. *ϕ represents α.*
2. *$\phi(X_1, \ldots, X_n) - \alpha\,Y^2$ is isotropic.*

Proof. (1) implies (2) obviously without assumption that ϕ is regular.
Now assume $\phi(\underline{X}) - \alpha\,Y^2$ is isotropic, meaning that there exist $(\underline{x}, y) \in K^{n+1}$ such that $\phi(\underline{x}) - \alpha\,y^2 = 0$.
If $y \neq 0$, then $y^{-2}\,\phi(\underline{x}) = \phi(y^{-1}\,\underline{x}) = \alpha$.
If $y = 0$, then $\underline{x} \neq 0$ and ϕ is isotropic (and regular), and thus universal. ■

Corollary 8.20. *Any quadratic form in ≥ 3 variables over a finite field is isotropic.*

Proof. We may assume that ϕ is diagonal and regular:

$$\phi(X_1, X_2, X_3) = \alpha_1\,X_1^2 + \alpha_2\,X_2^2 + \alpha_3\,X_3^2,$$

where $\alpha_1, \alpha_2, \alpha_3 \neq 0$.
Now $\alpha_1\,X_1^2 + \alpha_2\,X_2^2$ is universal. In particular, it represents $-\alpha_3$. ■

Proposition 8.21. *Let $f(\underline{X})$ and $g(\underline{Y})$ be regular quadratic forms over K. Suppose $f(\underline{X}) - g(\underline{Y})$ is isotropic. Then there exists $\alpha \in K^\times$ represented by both f and g.*

Proof. By assumption we have $(\underline{x}, \underline{y}) \neq (\underline{0}, \underline{0})$ such that $f(\underline{x}) = g(\underline{y}) = \beta$. Without loss of generality assume $\underline{x} \neq 0$. If $\beta \neq 0$, then we are done.
If $\beta = 0$, then $f(\underline{x}) = 0$, so f is isotropic, and thus universal, representing any element. We can take any element $\alpha \in K^\times$ represented by g. ■

Transforming orthogonal bases

Here we will show a technical result that will be used later in § 11.

Proposition 8.22. *Let (U, ϕ) be a quadratic space with two orthogonal bases $\widetilde{u} = (u_1, \ldots, u_n)$ and $\widetilde{v} = (v_1, \ldots, v_n)$. There exists a sequence of orthogonal bases*

$$\widetilde{u} = \widetilde{u}^{(0)}, \widetilde{u}^{(1)}, \widetilde{u}^{(2)}, \ldots, \widetilde{u}^{(\ell)} = \widetilde{v},$$

where $\widetilde{u}^{(i)}$ and $\widetilde{u}^{(i+1)}$ differ by at most two vectors.

Proof. For an induction step it is enough to transform $\widetilde{u} = (u_1, \dots, u_n)$ into some basis of the form $(v_1, v_2^*, \dots, v_n^*)$.

Write $v_1 = \alpha_1 u_1 + \dots + \alpha_n u_n$. Without loss of generality (after changing the order) we can assume $\alpha_1, \dots, \alpha_s \neq 0$ and $\alpha_{s+1}, \dots, \alpha_n = 0$, so that $v_1 = \alpha_1 u_1 + \dots + \alpha_s u_s$. We should have $\underline{\alpha} \neq \underline{0}$.

- If $s = 1$, then $v_1 = \alpha_1 u_1$, and we take $v_2^* = u_2, \dots, v_n^* = u_n$.
- If $s \geq 2$ and $\phi(\alpha_1 u_1 + \alpha_2 u_2) \neq 0$, consider $u_1' = \alpha_1 u_1 + \alpha_2 u_2$. Find u_2' of the form $\beta_1 u_1 + \beta_2 u_2$ such that $\psi(u_1', u_2') = 0$.

$$\begin{aligned}\psi(u_1', u_2') &= \psi(\alpha_1 u_1 + \alpha_2 u_2, \beta_1 u_1 + \beta_2 u_2) \\ &= \alpha_1 \beta_1 \psi(u_1, u_1) + \alpha_1 \beta_2 \underbrace{\psi(u_1, u_2)}_{=0} + \alpha_2 \beta_1 \underbrace{\psi(u_2, u_1)}_{=0} + \alpha_2 \beta_2 \psi(u_2, u_2) \\ &= \alpha_1 \beta_1 \phi(u_1) + \alpha_2 \beta_2 \phi(u_2).\end{aligned}$$

  So we take $\beta_1 = \alpha_2 \phi(u_2)$ and $\beta_2 = -\alpha_1 \phi(u_1)$. We have $(\beta_1, \beta_2) \neq (0,0)$ since $\phi(\alpha_1 u_1 + \alpha_2 u_2) = \alpha_1^2 \phi(u_1) + \alpha_2^2 \phi(u_2) \neq 0$.

  Consider a new basis $u_1', u_2', u_3, \dots, u_n$. We have $v_1 = u_1' + \alpha_3 u_3 + \dots + \alpha_s u_s$, a linear combination of $s-1$ vectors. So we reduced s to $s-1$, and we can use induction.
- If $s \geq 2$ and $\phi(\alpha_1 u_1 + \alpha_2 u_2) = 0$, then it is not possible for $s = 2$ (since $v_1 = \alpha_1 u_1 + \alpha_2 u_2$ is not isotropic), and we should have $s \geq 3$. Consider the following three vectors:

$$\begin{aligned}&\alpha_1 u_1 + \alpha_2 u_2, \\ &\alpha_1 u_1 + \alpha_3 u_3, \\ &\alpha_2 u_2 + \alpha_3 u_3.\end{aligned}$$

  We claim that at least one of them is not isotropic. Indeed, assume it is not the case. Then

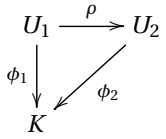
$$\begin{aligned}\alpha_1^2 \phi(u_1) + \alpha_2^2 \phi(u_2) &= 0, \\ \alpha_1^2 \phi(u_1) + \alpha_3^2 \phi(u_3) &= 0, \\ \alpha_2^2 \phi(u_2) + \alpha_3^2 \phi(u_3) &= 0.\end{aligned}$$

  But this implies $\alpha_1^2 = \alpha_2^2 = \alpha_3^2 = 0$, contradicting $\underline{\alpha} \neq \underline{0}$.

■

Witt's lemma

Definition 8.23. An **isometry** of quadratic spaces (U_1, ϕ_1) and (U_2, ϕ_2) is a linear map $\rho\colon U_1 \to U_2$ such that the following diagram commutes:



If there is an invertible isometry $\rho\colon U_1 \to U_2$, then we say that the quadratic spaces (U_1, ϕ_1) and (U_2, ϕ_2) are **isometric** and the corresponding quadratic forms ϕ_1 and ϕ_2 are **equivalent**.

For equivalent quadratic forms the discriminant is the same: if $\phi_1 \sim \phi_2$, then $\delta(\phi_1) = \delta(\phi_2)$ (as elements of $K^\times/(K^\times)^2$). Obviously the dimension of isometric quadratic spaces must be the same.

We will need the following important result:

Theorem 8.24 (Witt's lemma)**.** *Let $f_1(X_1,\dots,X_m)$, $f_2(X_1,\dots,X_m)$, $g_1(Y_1,\dots,Y_n)$, $g_2(Y_1,\dots,Y_n)$ be quadratic forms with f_1 and f_2 regular. Assume $f_1(\underline{X}) \sim f_2(\underline{X})$ and $f_1(\underline{X}) + g_1(\underline{Y}) \sim f_2(\underline{X}) + g_2(\underline{Y})$. Then $g_1(\underline{Y}) \sim g_2(\underline{Y})$.*

This essentially says that one has the "cancellation property" $f + g_1 = f + g_2 \Rightarrow g_1 = g_2$ for equivalence classes of quadratic forms. To prove this we need to discuss isometries of quadratic spaces.

An isometry (U,ϕ) to itself is called an **autoisometry**. That is, it is a map $\rho\colon U \to U$ such that $\phi \circ \rho = \phi$.

Suppose (U,ϕ) is regular. Then the autoisometries of (U,ϕ) are all invertible and they form a subgroup of $\mathrm{GL}(U)$, denoted by $O_\phi(U)$.

Proposition 8.25. *For $\rho \in O_\phi(U)$ one has* $\det\rho = \pm 1$.

Proof. Let $u_1,\dots,u_n$ be a basis of U. Consider the matrix $S = (\psi(u_i,u_j))_{i,j}$. If T is the matrix of ρ in this basis, then the matrix of $\phi\circ\rho$ is given by ${}^tTST = S$, and

$$\det({}^tTST) = (\det T)^2 \det S = \det S.$$

Since $\det S \neq 0$, we conclude $\det T = \pm 1$. ■

Consider a subgroup of $O_\phi(U)$ given by

$$O^+_\phi(U) := \{\rho \in O_\phi(U) \mid \det\rho = +1\}.$$

We have $[O_\phi(U) : O^+_\phi(U)] = 2$. Indeed, the index is either 1 or 2, and we can find an element $\rho \in O_\phi(U)$ with $\det\rho = -1$. (As before, we assume $\mathrm{char}\, K \neq 2$, otherwise $+1 = -1$.)

Example 8.26. Take u such that $\phi(u) \neq 0$. We have $U = \langle u\rangle + \langle u\rangle^\perp$. Define a map

$$\begin{aligned} \rho_u\colon U &\to U,\\ u &\mapsto -u,\\ v &\mapsto 1 \quad \text{for } v \in \langle u\rangle^\perp. \end{aligned}$$

We have $\det\rho_u = -1$.

In general, the reflection through the hyperplane orthogonal to u is given by

$$\rho_u(v) = v - 2\frac{\psi(u,v)}{\psi(u,u)}\,u.$$

("Reflection" is understood with respect to the bilinear form ψ.)

In particular, if $\phi(u) = \phi(v)$ and $\phi(u-v) \neq 0$, then

$$\rho_{u-v}(u) = v, \quad \rho_{u-v}(v) = u.$$

Indeed, by the definition of reflection

$$\rho_{u-v}(u) := u - 2\frac{\psi(u-v,u)}{\psi(u-v,u-v)}\,(u-v).$$

By bilinearity,

$$\psi(u-v,u) = \psi(u,u) - \psi(v,u).$$

By bilinearity together with the assumption $\phi(u) = \phi(v)$,

$$\psi(u-v, u-v) = \psi(u,u) - 2\psi(v,u) + \psi(v,v) = 2(\psi(u,u) - \psi(v,u)),$$

hence

$$\rho_{u-v}(u) := u - 2\frac{\psi(u-v,u)}{\psi(u-v,u-v)}(u-v) = u - (u-v) = v.$$

▲

Proposition 8.27. *Suppose $u, v \in U$ are such that $\phi(u) = \phi(v) \neq 0$. Then there exists $\rho \in O_\phi(U)$ such that $\rho(u) = v$.*

Proof.

- If $\phi(u-v) \neq 0$, then take a reflection $\rho_{u-v}(u) = v$.
- If $\phi(u+v) \neq 0$, then we have a reflection $\rho_{u+v}(u) = -v$ and we take its composition with another reflection: $\rho_v \rho_{u+v}(u) = v$.
- We claim that both $\phi(u-v)$ and $\phi(u+v)$ cannot be zero under our assumptions. Indeed,

$$\phi(u+v) + \phi(u-v) = 2\phi(u) + 2\phi(v) = 4\phi(v) \neq 0.$$

■

If $\dim U > 1$, then in the proposition above we may actually take ρ to be a product of two reflections, so that $\rho \in O^+_\phi(U)$. Indeed, in this case there exists $w \perp u$ such that $\phi(w) \neq 0$, and

- $\rho_{u-v}\rho_w(u) = v$ if $\phi(u-v) \neq 0$—this is because $\rho_w(u) = u$, since we reflect u with respect to the hyperplane orthogonal to w, but u is in that hyperplane;
- $\rho_v \phi_{u+v}(u) = v$ as before if $\phi(u+v) \neq 0$.

Theorem 8.28. *Assume $V_1, V_2 \subseteq U$ are two regular quadratic subspaces of U and they are isometric via some $\rho\colon V_1 \to V_2$. Then this ρ can be extended to an autoisometry of U.*

Proof. Since V_1 is regular, there exists $v_1 \in V_1$ such that $\phi(v_1) \neq 0$. By proposition 8.27 there exists $\sigma \in O_\phi(U)$ such that $\sigma(\rho(v_1)) = v_1$. We may replace V_2 with σV_2 and ρ with $\sigma\rho$, so that $v_1 \in V_1 \cap V_2$ and $\rho(v_1) = v_1$.

For $\dim V_1 = 1$ we are done. Otherwise we use induction on $\dim V_1$. Consider

$$U' := \langle v \rangle^\perp, \quad V_1' = U' \cap V_1, \quad V_2' = U' \cap V_2.$$

We have $\dim V_1' = \dim V_1 - 1$ and $\dim V_2' = \dim V_2 - 1$ and $\rho V_1' = V_2'$. By induction hypothesis, there is an autoisometry ρ' of U' such that $\rho'\big|_{V_1} = \rho$. From this we can define an autoisometry on the whole U by

$$\begin{aligned} \sigma\colon U &\to U, \\ v &\mapsto v, \\ u &\mapsto \rho'(u) \quad \text{for } u \in U'. \end{aligned}$$

■

Corollary 8.29. *Assume U_1 and U_2 are isometric quadratic spaces and $V_1 \subseteq U_1$, $V_2 \subseteq U_2$, with V_1, V_2 regular and isometric subspaces. Then $V_1^\perp$ is isometric to $V_2^\perp$.*

Proof. By assumption there is an isometry $\rho\colon U_1 \to U_2$ is an isometry. We can replace U_1 with ρU_1 and V_1 with ρV_1, and assume that $(U_1, \phi_1) = (U_2, \phi_2) = (U, \phi)$ is a single quadratic space and V_1 and V_2 are its regular subspaces isometric via some $\rho\colon V_1 \to V_2$. Then we know by the previous theorem that the is an autoisometry σ extending ρ. But then $\sigma V_1 = V_2$ and $\sigma V_1^\perp = V_2^\perp$. ■

This corollary proves the Witt's lemma (theorem 8.24). Indeed, assume we have equivalent quadratic forms

$$f_1(X_1,\dots,X_m)+g_1(Y_1,\dots,Y_n)\sim f_2(X_1,\dots,X_m)+g_2(Y_1,\dots,Y_n),$$

with f_1 and f_2 regular and equivalent. Consider a quadratic space U_1 having quadratic form $f_1(\underline{X})+g_1(\underline{Y})$ and a quadratic space U_2 having quadratic form $f_2(\underline{X})+g_2(\underline{Y})$. Then f_1 and f_2 correspond to regular isometric subspaces $V_1\subset U_1$ and $V_2\subset U_2$. The quadratic forms g_1 and g_2 correspond to subspaces $V_1^{\perp}$ and $V_2^{\perp}$ that should be isometric as well. ■

9 Quadratic forms over $\mathbb{Q}_p$

Proposition 9.1. *Suppose $p>2$ is a finite prime and ϕ is a regular quadratic form over $\mathbb{Q}_p$.*

1. *Suppose the dimension is ≥ 3. If ϕ has a diagonal form*

$$\phi=\alpha_1 X_1^2+\alpha_2 X_2^2+\alpha_3 X_3+\cdots$$

with $\alpha_1,\alpha_2,\alpha_3$ being units (equivalently, $\nu_p(\alpha_i)=0$), then ϕ is isotropic.

2. *Any quadratic form over $\mathbb{Q}_p$ of dimension ≥ 5 is isotropic.*

We note now that the first assertion is false for $p=2$ (a counterexample will follow, see p. 28). The second assertion is still true for $p=2$, and we will see a proof of this later (theorem 11.2).

Proof. 1. It is a typical application of Hensel. There exists $\underline{a}=(a_1,a_2,a_3)$ such that $\underline{a}\neq 0$ and $\phi(\underline{a})\equiv 0 \pmod p$, because over $\mathbb{F}_p$ any quadratic form of dimension ≥ 3 is isotropic. Without loss of generality assume $a_1\neq 0$. Then $\phi'_{X_1}(\underline{a})=2a_1\not\equiv 0 \pmod p$ (and here we use the assumption $p\neq 2$). Now by the Hensel's lemma (theorem 6.7) there exists $\underline{b}\in\mathbb{Z}_p^3$ such that $\underline{b}\equiv\underline{a}\not\equiv 0 \pmod p$ and $\phi(\underline{b})=0$.

2. We may assume $n=5$ and that $\phi=\alpha_1 X_1^2+\cdots+\alpha_5 X_5^2$. Also without loss of generality (by multiplying by p^k and applying a variable change) $\nu_p(\alpha_i)\in\{0,1\}$. Thus $\phi=\phi_1+p\phi_2$, where the coefficients of ϕ_1 and ϕ_2 are units. Now $\dim\phi_1\geq 3$ or $\dim\phi_2\geq 3$, so we have isotropy by the previous proposition (that is why we ask that $p\neq 2$, but this restriction can be removed).

■

10 Hilbert symbol

From now on p denotes a prime, possibly 2 or infinite.

Definition 10.1. Let $\alpha,\beta\in\mathbb{Q}_p^{\times}$. The **Hilbert symbol** $(\alpha,\beta)_p$ is defined as follows:

$$(\alpha,\beta)_p:=\begin{cases}+1, & \alpha X^2+\beta Y^2-Z^2 \text{ is isotropic,}\\ -1, & \alpha X^2+\beta Y^2-Z^2 \text{ is anisotropic.}\end{cases}$$

In the definition above "$\alpha X^2+\beta Y^2-Z^2$ is isotropic" can be replaced with "$Z^2-\alpha X^2$ represents β". Indeed, suppose $\alpha x^2+\beta y^2-z^2=0$ for some $(x,y,z)\neq(0,0,0)$. If $y=0$ then $Z^2-\alpha X^2$ is isotropic, and thus universal, so it represents β. If $y\neq 0$, then we get

$$(z/y)^2-\alpha(x/y)^2=\beta,$$

so the form $Z^2-\alpha X^2$ indeed represents β.

Here are some immediate properties of the Hilbert symbol:

1. $(\alpha,\beta)_p=(\beta,\alpha)_p$.

2. $(\alpha, -\alpha)_p = 1$ (for this observe that $\alpha X^2 - \alpha Y^2 - Z^2$ is isotropic; take $X = Y = 1$ and $Z = 0$).

3. $(\alpha, 1)_p = 1$ (since $\alpha X^2 + Y^2 - Z^2$ is isotropic; take $X = 0$, $Y = Z = 1$).

4. $(\alpha, \gamma^2\beta)_p = (\alpha, \beta)_p$ (one can make a variable change $Y' := Y/\gamma$).

5. $(\alpha, \gamma^2)_p = (\alpha, 1)_p = 1$.

There is one more equivalent definition of the Hilbert symbol:

$$(\alpha, \beta)_p = 1 \iff \beta \text{ is a norm of some element in } \mathbb{Q}_p(\sqrt{\alpha})/\mathbb{Q}_p.$$

Indeed, if $\alpha \in (\mathbb{Q}_p^\times)^2$, then this is trivial and the symbol $(\alpha, \beta)_p$ is always 1, just as for the definition above. Now if $\alpha \notin (\mathbb{Q}_p^\times)^2$, then for an arbitrary element $z + x\sqrt{\alpha} \in \mathbb{Q}_p(\alpha)^\times$ we compute its norm

$$N_{\mathbb{Q}_p(\sqrt{\alpha})/\mathbb{Q}_p}(z + x\sqrt{\alpha}) = \det \begin{pmatrix} z & \alpha x \\ x & z \end{pmatrix} = z^2 - \alpha x^2.$$

So it is the same as asking β to be represented by $Z^2 - \alpha X^2$ (even though the symmetry between α and β becomes less evident this way).

Proposition 10.2. *Hilbert symbol is multiplicative with respect to each variable:*

$$(\alpha_1\alpha_2, \beta)_p = (\alpha_1, \beta)_p \cdot (\alpha_2, \beta)_p,$$
$$(\alpha, \beta_1\beta_2)_p = (\alpha, \beta_1)_p \cdot (\alpha, \beta_2)_p.$$

We will first show the following:

Proposition 10.3. *Fix α. Then $G_\alpha := \{\beta \mid (\alpha, \beta)_p = 1\}$ is a subgroup of $\mathbb{Q}_p^\times$ of index 1 or 2.*

The proposition 10.2 follows easily from the proposition 10.3. Suppose G_α is a group of index one or two. For $\beta_1, \beta_2 \in \mathbb{Q}_p$ We have the following three cases:

1. $\beta_1, \beta_2 \in G_\alpha$. Then $(\alpha, \beta_1)_p \cdot (\alpha, \beta_2)_p = (\alpha, \beta_1\beta_2)_p = 1$.

2. $\beta_1 \in G_\alpha$, $\beta_2 \notin G_\alpha$. Then $(\alpha, \beta_1)_p = 1$ and $(\alpha, \beta_2)_p = (\alpha, \beta_1\beta_2)_p = -1$.

3. $\beta_1, \beta_2 \notin G_\alpha$. Then since $[\mathbb{Q}_p^\times : G_\alpha] \le 2$, one must have $\beta_1\beta_2 \in G_\alpha$. So $(\alpha, \beta_1)_p = (\alpha, \beta_2)_p = -1$ and $(\alpha, \beta_1\beta_2)_p = 1$. ∎

Proof of the proposition 10.3. If $\alpha \in (\mathbb{Q}_p^\times)^2$ then $(\alpha, \beta)_p = 1$ for all $\beta \in \mathbb{Q}_p^\times$, and we have nothing to prove (in this case $G_\alpha = \mathbb{Q}_p^\times$).

So we may assume $\alpha \notin (\mathbb{Q}_p^\times)^2$, in which case $[\mathbb{Q}_p(\sqrt{\alpha}) : \mathbb{Q}_p] = 2$. The norm $N_{\mathbb{Q}_p(\sqrt{\alpha})/\mathbb{Q}_p}$ is a homomorphism $\mathbb{Q}_p(\sqrt{\alpha})^\times \to \mathbb{Q}_p^\times$, so it is clear that its image, which is G_α, is a subgroup in $\mathbb{Q}_p^\times$. Our goal is to show that the index of this subgroup is 1 or 2.

From the properties above we see that $(\mathbb{Q}_p^\times)^2 \subseteq G_\alpha$, where $(\mathbb{Q}_p^\times)^2$ is the group of squares in $\mathbb{Q}_p^\times$. So the index $[\mathbb{Q}_p^\times : G_\alpha]$ should divide the index $[\mathbb{Q}_p^\times : (\mathbb{Q}_p^\times)^2]$, and the latter is

- 2 for $p = \infty$;
- 4 for $2 < p < \infty$;
- 8 for $p = 2$.

In case $p=\infty$ we are done. The index is

$$[\mathbb{Q}_\infty^\times : G_\alpha] = \begin{cases} 1, & \text{if } \alpha > 0, \\ 2, & \text{if } \alpha < 0. \end{cases}$$

Now for $2 < p < \infty$ we show that $[\mathbb{Q}_p^\times : G_\alpha] = 2$. It is enough to find an element $\beta \in G_\alpha$ such that $\beta \notin (\mathbb{Q}_p^\times)^2$ (which would prove $[\mathbb{Q}_p^\times : G_\alpha] \neq 4$) and another $\beta \in \mathbb{Q}_p^\times$ such that $\beta \notin G_\alpha$ (which would prove $[\mathbb{Q}_p^\times : G_\alpha] \neq 1$).

Since we consider α modulo squares, we may assume that $\nu_p(\alpha) = 0$ or 1.

- In case $\nu_p(\alpha) = 0$ for each β with $\nu_p(\beta) = 0$ the form $\alpha X^2 + \beta Y^2 - Z^2$ is isotropic (all coefficients are units), so $\mathbb{Z}_p^\times \subseteq G_\alpha$. Now for α being a unit also $-\alpha$ is a unit, so $-\alpha \in G_\alpha$. On the other hand, $-\alpha \notin (\mathbb{Q}_p^\times)^2$.

  If $\nu_p(\alpha) = 0$, then the form $\alpha X^2 + p Y^2 - Z^2$ is anisotropic. Indeed, otherwise $\alpha X^2 - Z^2$ would be isotropic modulo p, but α is not a square modulo p. Thus $p \notin G_\alpha$.

- If $\nu_p(\alpha) = 1$, then $\alpha = p\eta$ for some unit η. Take a unit $\gamma \in \mathbb{Z}_p^\times$ which is not a square in $\mathbb{Z}_p^\times$. We claim that the form $p\eta X^2 + \gamma Y^2 - Z^2$ is anisotropic and so $\gamma \notin G_\alpha$. Indeed, if it is isotropic, then $\gamma Y^2 - Z^2$ is isotropic modulo p, but γ is not a square.

So we conclude that $[\mathbb{Q}_p^\times : G_\alpha] = 2$ for $2 < p < \infty$.

Finally, for $p = 2$ a similar analysis gives $[\mathbb{Q}_p^\times : G_\alpha] = 2$. ■

Now we can write down the values of the Hilbert symbol $(\cdot,\cdot)_p$ for various p. In case $p=\infty$ the form (over the field $\mathbb{R}$ of real numbers) $\alpha X^2 + \beta Y^2 - Z^2$ is anisotropic iff $\alpha < 0$ and $\beta < 0$, so

$$(\alpha,\beta)_\infty = \begin{cases} +1, & \alpha > 0 \text{ or } \beta > 0, \\ -1, & \alpha < 0 \text{ and } \beta < 0. \end{cases}$$

We summarize it in the following table:

$\mathbb{R}$	$+1$	-1
$+1$	$+1$	$+1$
-1	$+1$	-1

Now assume $2 < p < \infty$. The subgroup of squares $(\mathbb{Q}_p^\times)^2$ in $\mathbb{Q}_p^\times$ has four cosets represented by $1, \epsilon, p, p\epsilon$, where ϵ is some nonsquare unit in $\mathbb{Z}_p^\times$.

- If both α and β are units then $\alpha X^2 + \beta Y^2 - Z^2$ is isotropic, so $(\alpha,\beta)_p = 1$.

- If α is a unit then $(\alpha, p)_p = \left(\frac{\alpha}{p}\right)$, the **Legendre symbol**

$$\left(\frac{\alpha}{p}\right) := \begin{cases} +1, & \text{if } \alpha \text{ is a square} \quad \mod p, \\ 0, & \text{if } \alpha \equiv 0 \quad \mod p, \\ -1, & \text{if } \alpha \text{ is not a square} \quad \mod p. \end{cases}$$

  This is because $\alpha X^2 + p Y^2 - Z^2$ is isotropic *iff* $\alpha X^2 - Z^2$ is isotropic modulo p.

- $(p,p)_p = (p,-p)_p \cdot (p,-1)_p = (p,-1)_p = \left(\frac{-1}{p}\right)$.

- By multiplicativity $(p\epsilon,\epsilon)_p = (p,\epsilon)_p \cdot (\epsilon,\epsilon)_p = (p,\epsilon)_p = \left(\frac{\epsilon}{p}\right) = -1$, since ϵ is a nonsquare in $\mathbb{Z}_p^\times$.

- Similarly $(p,p\epsilon)_p = (p,\epsilon)_p \cdot (p,p)_p = \left(\frac{\epsilon}{p}\right) \cdot \left(\frac{-1}{p}\right) = \left(\frac{-\epsilon}{p}\right) = -\left(\frac{-1}{p}\right)$.

- Finally, $(p\epsilon,p\epsilon)_p = (p\epsilon,p)_p \cdot (p\epsilon,\epsilon)_p = \left(\frac{-\epsilon}{p}\right) \cdot \left(\frac{\epsilon}{p}\right) = \left(\frac{-1}{p}\right)$.

We summarize our computations in the following table:

$\mathbb{Q}_p$	1	ϵ	p	$p\epsilon$
1	$+1$	$+1$	$+1$	$+1$
ϵ	$+1$	$+1$	-1	-1
p	$+1$	-1	$+\left(\frac{-1}{p}\right)$	$-\left(\frac{-1}{p}\right)$
$p\epsilon$	$+1$	-1	$-\left(\frac{-1}{p}\right)$	$+\left(\frac{-1}{p}\right)$

Recall that

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1, & p \equiv 1 \pmod 4, \\ -1, & p \equiv 3 \pmod 4. \end{cases}$$

A similar table can be constructed for $p = 2$. Recall that $\mathbb{Z}_2^\times/(\mathbb{Z}_2^\times)^2$ can be identified with $(\mathbb{Z}/8\mathbb{Z})^\times$, which is represented by residues $\{\overline{1},\overline{3},\overline{5},\overline{7}\}$ modulo 8 (multiplicatively these form a group isomorphic to $C_2 \times C_2$). The group $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ is represented by numbers $\{1,3,5,7,2,6,10,14\}$. Investigating the values $(\alpha,\beta)_2$ for all $\alpha,\beta \in \{1,3,5,7,2,6,10,14\}$, one can obtain

$\mathbb{Q}_2$	1	3	5	7	2	6	10	14
1	$+1$	$+1$	$+1$	$+1$	$+1$	$+1$	$+1$	$+1$
3	$+1$	-1	$+1$	-1	-1	$+1$	-1	$+1$
5	$+1$	$+1$	$+1$	$+1$	-1	-1	-1	-1
7	$+1$	-1	$+1$	-1	$+1$	-1	$+1$	-1
2	$+1$	-1	-1	$+1$	$+1$	-1	-1	$+1$
6	$+1$	$+1$	-1	-1	-1	-1	$+1$	$+1$
10	$+1$	-1	-1	$+1$	-1	$+1$	$+1$	-1
14	$+1$	$+1$	-1	-1	$+1$	$+1$	-1	-1

To understand how one can compile such a table, see below the characterization of isotropic ternary forms over $\mathbb{Q}_2$.

One could start with defining the Hilbert symbol as a function on $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ given by such tables and prove all its properties by routine verifications. However, it would not be very instructive.

Product formula

Fix $\alpha,\beta \in \mathbb{Q}^\times$. Observe that $(\alpha,\beta)_p = 1$ for all but finitely many p because if p is odd and $\alpha,\beta \in \mathbb{Z}_p^\times$, then $(\alpha,\beta)_p = 1$. So the product $\prod_p (\alpha,\beta)_p$ is well-defined.

Theorem 10.4 (Product formula)**.**

$$\prod_{2 \le p \le \infty} (\alpha,\beta)_p = 1.$$

In other words, $(\alpha,\beta)_p = -1$ *for even number of* p*'s.*

Example 10.5. Consider $(5,14)_p$. One has

$$
\begin{aligned}
(6,14)_2 &= 1,\\
(6,14)_3 &= (2,2)_3\cdot(2,7)_3\cdot(3,2)_3\cdot(3,7)_3 = 1\cdot 1\cdot(-1)\cdot 1 = -1,\\
(6,14)_5 &= 1,\\
(6,14)_7 &= (2,2)_7\cdot(2,7)_7\cdot(3,2)_7\cdot(3,7)_7 = 1\cdot 1\cdot 1\cdot(-1) = -1,\\
(6,14)_{11} &= 1,\\
&\cdots\\
(6,14)_\infty &= 1.
\end{aligned}
$$

▲

An analogue of this product formula is the product formula for valuations on a global field K (generalizing theorem 4.14); see p. 61.

First we derive a corollary from theorem 10.4:

Corollary 10.6. *Let ϕ be a ternary quadratic form over $\mathbb{Q}$. Then the set*

$$\{p \mid \phi \text{ is anisotropic over } \mathbb{Q}_p\}$$

is finite and has even cardinality.

Proof. If ϕ is not regular, then ϕ is always isotropic.

If ϕ is regular, then it has form $\gamma(\alpha X^2+\beta Y^2-Z^2)$, and the latter is anisotropic iff $(\alpha,\beta)_p=-1$. ■

Proof of theorem 10.4. Since the Hilbert symbol $(\alpha,\beta)_p$ is multiplicative in both variables, we may consider only the following cases:

- $\alpha=-1$, $\beta=-1$,
- $\alpha=-1$, $\beta=2$,
- $\alpha=-1$, $\beta=q$ an odd prime,
- $\alpha=2$, $\beta=2$,
- $\alpha=2$, $\beta=q$,
- $\alpha=q$, $\beta=q$,
- $\alpha=q$, $\beta=q'$ with $q\neq q'$.

Since $(\alpha,\alpha)_p=(\alpha,-1)_p$, the cases $(2,2)_p$ and $(q,q)_p$ reduce to the other ones.

1. Let $\alpha=-1$, $\beta=-1$. For $2<p<\infty$ we have $(-1,-1)_p=1$. For $p=\infty$ we have $(-1,-1)_\infty=-1$.

   Finally, to compute $(-1,-1)_2$, observe that the quadratic form $-X^2-Y^2-Z^2$ is anisotropic over $\mathbb{Q}_2$. Indeed, if it is isotropic, then we have a nonzero triple $x,y,z\in\mathbb{Z}_2$ such that $x^2+y^2+z^2=0$. We may assume $\gcd(x,y,z)=1$, so, say, x and y are odd and z is even. But now $x^2+y^2+z^2\equiv 2 \pmod 4$, which is a contradiction.

   $$\prod_{2\le p\le\infty}(-1,-1)_p=(-1,-1)_\infty\cdot(-1,-1)_2=1.$$

   Now let us make a little deviation to see when in general quadratic forms over $\mathbb{Q}_2$ are isotropic. We just seen that $X^2+Y^2+Z^2$ is anisotropic over $\mathbb{Q}_2$, which shows that the first assertion of proposition 9.1 is wrong for $p=2$.

   Let $\phi=\alpha X^2+\beta Y^2+\gamma Z^2$ be a quadratic form. We may assume $v_2(\alpha),v_2(\beta),v_2(\gamma)\in\{0,1\}$. We have two cases: either $\alpha,\beta,\gamma\in\mathbb{Z}_2^\times$ or $\alpha,\beta\in\mathbb{Z}_2^\times$, $\gamma\in 2\mathbb{Z}_2^\times$.

- If α, β, γ are all units, then assume there is $(x,y,z) \in \mathbb{Z}_2^3$, $(x,y,z) \neq \underline{0}$ such that $\alpha x^2 + \beta y^2 + \gamma z^2 = 0$. Two of x, y, z are odd and one is even, e.g. x and y are odd and z is even. Then $\alpha + \beta \equiv 0 \pmod 4$. Similarly for the other combinations x, z and y, z, we get

$$\phi \text{ isotropic} \iff \left\{ \begin{array}{c} \alpha + \beta \equiv 0 \pmod 4 \\ \text{or} \\ \alpha + \gamma \equiv 0 \pmod 4 \\ \text{or} \\ \beta + \gamma \equiv 0 \pmod 4 \end{array} \right\}$$

  We would like to show the opposite implication "$\Leftarrow$". Assume, say, $\alpha + \beta \equiv 0 \pmod 4$. Then either $\alpha + \beta \equiv 0 \pmod 8$ or $\alpha + \beta \equiv 4 \pmod 8$.

  If $\alpha + \beta \equiv 0 \pmod 8$, take $x_0 = 1, y_0 = 1, z_0 = 0$. We have $\phi(x_0, y_0, z_0) \equiv 0 \pmod 8$ and $\phi'_X(x_0, y_0, z_0) \not\equiv 0 \pmod 4$. So the Hensel's lemma (theorem 6.7) provides us the desired (x, y, z), and ϕ is isotropic.

  If $\alpha + \beta \equiv 4 \pmod 8$, then similarly we can take $x_0 = 1, y_0 = 1, z_0 = 2$.

- Suppose α and β are units and $\gamma \in 2\mathbb{Z}_2^\times$. By an argument similar to the one above we can show that

$$\phi \text{ isotropic} \iff \left\{ \begin{array}{c} \alpha + \beta \equiv 0 \pmod 8 \\ \text{or} \\ \alpha + \beta + \gamma \equiv 0 \pmod 8 \end{array} \right\}$$

2. Let $\alpha = -1$, $\beta = 2$.

   We compute $(-1,2)_\infty = 1$ and $(-1,2)_p = 1$ for $2 < p \leq \infty$ since $-X^2 + 2Y^2 - Z^2$ is isotropic (has units as its coefficients). On the other hand, $-X^2 + 2Y^2 - Z^2$ is also isotropic over $\mathbb{Q}_2$. So $(-1,2)_p = 1$ for each prime p, and the product formula holds.

3. Let $\alpha = -1$, $\beta = q$ an odd prime.

   The form $-X^2 + qY^2 - Z^2$ is isotropic for $2 < p < \infty$ and $p \neq q$, so $(-1, q)_p = 1$. For $p = q$ the form is isotropic iff $X^2 + Z^2$ is isotropic modulo q, which happens whenever -1 is a square modulo q. So $(-1, q)_q = \left(\frac{-1}{q}\right)$.

   Over $\mathbb{R}$ the form $-X^2 + qY^2 - Z^2$ is isotropic, and over $\mathbb{Q}_2$ it is isotropic iff $q \equiv 1 \pmod 4$, so $(-1, q)_2 = \left(\frac{-1}{q}\right)$. Finally we have

$$\prod_p (-1, q)_p = \left(\frac{-1}{q}\right) \cdot \left(\frac{-1}{q}\right) = 1.$$

   The case $\alpha = 2$, $\beta = q$ can be checked similarly.

4. Let $\alpha = q$, $\beta = q'$ with $q \neq q'$.

   Consider the form $qX^2 + q'Y^2 - Z^2$. It is isotropic over $\mathbb{R}$, and it is also isotropic over $\mathbb{Q}_p$ whenever $p \neq q, q'$ and $2 < p < \infty$.

   Now, as we seen above, $qX^2 + q'Y^2 - Z^2$ is isotropic over $\mathbb{Q}_2$ iff

$$q + q' \equiv 0 \pmod 4 \quad \text{or} \quad q - 1 \equiv 0 \pmod 4 \quad \text{or} \quad q' - 1 \equiv 0 \pmod 4.$$

   The first congruence is not the case for q and q' being distinct primes; so $qX^2 + q'Y^2 - Z^2$ is isotropic over $\mathbb{Q}_2$ iff q or q' is 1 modulo 4, giving

$$(q, q')_2 = (-1)^{\frac{q-1}{2}\frac{q'-1}{2}}.$$

Further, $qX^2 + q'Y^2 - Z^2$ is isotropic over $\mathbb{Q}_q$ if $q'Y^2 - Z^2$ is isotropic over $\mathbb{F}_q$, so

$$(q,q')_q = \left(\frac{q'}{q}\right), \quad (q,q')_{q'} = \left(\frac{q}{q'}\right).$$

Finally the product formula becomes

$$\prod_{2\le p\le\infty} (q,q')_p = (-1)^{\frac{q-1}{2}\frac{q'-1}{2}} \left(\frac{q'}{q}\right)\cdot\left(\frac{q}{q'}\right).$$

The latter expression is 1 by the **quadratic reciprocity law**.

■

The most interesting case in the proof above is of $(q,q')_p$ with $q \neq q'$, and we see that the product formula for the Hilbert symbol is equivalent in a certain sense to the quadratic reciprocity law.

11 Hasse invariant

Let ϕ be a regular quadratic form over $\mathbb{Q}_p$. We know two of its invariants: the dimension $\dim\phi$ (the number of variables) and the discriminant $\delta(\phi) \in \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$. We are going to define the third invariant of ϕ.

Write ϕ in a diagonal form

$$\phi = \alpha_1 X_1^2 + \alpha_2 X_2^2 + \cdots + \alpha_n X_n^2.$$

Define the **Hasse invariant** of ϕ to be

$$c(\phi) := \prod_{1\le i<j\le n} (\alpha_i, \alpha_j)_p.$$

We claim that it is indeed an invariant:

Theorem 11.1. *$c(\phi)$ does not depend on diagonalization of ϕ.*

Further, the Hasse invariant reflects the property of a quadratic form to be isotropic.

Theorem 11.2. *Let p be a finite prime (possibly 2). Let ϕ be a regular quadratic form over $\mathbb{Q}_p$ in n variables.*

1. *If $n = 2$, then ϕ is isotropic iff $\delta(\phi) = -1$ in $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$, i.e. whenever $-\delta(\phi)$ is a square.*
2. *If $n = 3$, then ϕ is isotropic iff $c(\phi) = (-1, -\delta(\phi))_p$.*
3. *If $n = 4$, then ϕ is anisotropic iff $c(\phi) = (-1,-1)_p$ and $\delta(\phi) \in (\mathbb{Q}_p^\times)^2$, i.e. is a square.*
4. *If $n \ge 5$, then ϕ is always isotropic.*

Finally, we will not prove it in these notes, but it is true that $\dim\phi$, $\delta(\phi)$, and $c(\phi)$ together give a full system of invariants for quadratic forms over $\mathbb{Q}_p$ with p being a finite prime.

Lemma 11.3. *Let ϕ be a regular binary form. Then ϕ is isotropic iff $\delta(\phi) = -1$ in $K^\times/(K^\times)^2$.*

Proof. We may consider $\phi = \alpha X^2 + \beta Y^2$. Then $\delta(\phi) = \alpha\beta$. Now ϕ is isotropic iff $\alpha\phi$ is isotropic, and $\alpha\phi$ is equivalent to $X^2 + \delta(\phi)Y^2$. The latter is isotropic iff $-\delta(\phi)$ is a square. ■

Lemma 11.4. *Let ϕ be a binary form over $\mathbb{Q}_p$. Then there exists $\epsilon = \epsilon(\phi) \in \{\pm 1\}$ such that*

$$\beta \in \mathbb{Q}_p^\times \text{ is represented by } \phi \iff (\beta, -\delta(\phi))_p = \epsilon.$$

Proof. We may assume that $\phi = \alpha_1 X_1^2 + \alpha_2 X_2^2$ is in diagonal form. Now β is represented by ϕ iff $\phi - \beta Y^2$ is isotropic, which is the same as $\frac{\alpha_1}{\beta} X_1^2 + \frac{\alpha_2}{\beta} X_2^2 - Y^2$ being isotropic. We compute the corresponding Hilbert symbol:

$$\left(\frac{\alpha_1}{\beta}, \frac{\alpha_2}{\beta}\right)_p = (\alpha_1, \alpha_2)_p \cdot \left(\alpha_1, \frac{1}{\beta}\right)_p \cdot \left(\frac{1}{\beta}, \alpha_2\right)_p \cdot \left(\frac{1}{\beta}, \frac{1}{\beta}\right)_p.$$

Since $(\beta, \gamma)_p \cdot (1/\beta, \gamma)_p = (1, \gamma)_p = 1$, we can replace $1/\beta$ with β:

$$\left(\frac{\alpha_1}{\beta}, \frac{\alpha_2}{\beta}\right)_p = (\alpha_1, \alpha_2)_p \cdot \left(\alpha_1, \beta\right)_p \cdot \left(\beta, \alpha_2\right)_p \cdot \left(\beta, \beta\right)_p.$$

Now observing that $\left(\beta, \beta\right)_p = (\beta, -\beta)_p \cdot (\beta, -1)_p = \left(\beta, -1\right)_p$, we get

$$\left(\frac{\alpha_1}{\beta}, \frac{\alpha_2}{\beta}\right)_p = (\alpha_1, \alpha_2)_p \cdot (\beta, -\alpha_1\alpha_2)_p = (\alpha_1, \alpha_2)_p \cdot (\beta, -\delta(\phi))_p.$$

So we see that β is represented by ϕ iff $(\beta, -\delta(\phi))_p = (\alpha_1, \alpha_2)_p$. ∎

- From the proof we see that $(\alpha_1, \alpha_2)_p$ is the same for any diagonalization of ϕ. In particular, $c(\phi)$ is well-defined for binary forms.
- The proof shows that the number ϵ in the lemma is actually $c(\phi)$.

Now we are ready to prove theorem 11.1. We have to show that if two forms $f := \alpha_1 X_1^2 + \cdots + \alpha_n X_n^2$ and $g := \beta_1 X_1^2 + \cdots + \beta_n X_n^2$ are equivalent, then

$$\prod_{i<j} (\alpha_i, \alpha_j)_p = \prod_{i<j} (\beta_i, \beta_j)_p.$$

We may assume that $\alpha_i = \beta_i$ for all i, with at most two exceptions (cf. proposition 8.22):

$$f = \alpha_1 X_1^2 + \alpha_2 X_2^2 + \alpha_3 X_3^2 + \cdots + \alpha_n X_n^2,$$
$$g = \beta_1 X_1^2 + \beta_2 X_2^2 + \alpha_3 X_3^2 + \cdots + \alpha_n X_n^2.$$

By Witt's lemma (theorem 8.24), if $f \sim g$, then $\alpha_1 X_1^2 + \alpha_2 X_2^2 \sim \beta_1 X_1^2 + \beta_2 X_2^2$, and so from the proof of lemma 11.4 we know that $(\alpha_1, \alpha_2)_p = (\beta_1, \beta_2)_p$. Moreover, $\alpha_1\alpha_2 = \beta_1\beta_2$ modulo squares $(\mathbb{Q}_p^\times)^2$.

$$\prod_{i<j} (\alpha_i, \alpha_j)_p = (\beta_1, \beta_2)_p \cdot \prod_{j\geq 3} (\alpha_1\alpha_2, \alpha_j)_p \cdot \prod_{3\leq i<j\leq n} (\alpha_i, \alpha_j)_p = (\beta_1, \beta_2)_p \cdot \prod_{j\geq 3} (\beta_1\beta_2, \beta_j)_p \cdot \prod_{3\leq i<j\leq n} (\beta_i, \beta_j)_p = \prod_{i<j} (\beta_i, \beta_j)_p.$$

∎

So the Hasse invariant is indeed an invariant of a quadratic form.

Lemma 11.5. *Let $f(\underline{X}) = f(X_1, \ldots, X_m)$ and $g(\underline{Y}) = g(Y_1, \ldots, Y_n)$ be two quadratic forms. Then for their sum $f(\underline{X}) + g(\underline{Y})$ (as a quadratic form in $X_1, \ldots, X_m, Y_1, \ldots, Y_n$) holds*

$$\begin{aligned} \dim(f+g) &= \dim f + \dim g, \\ \delta(f+g) &= \delta(f) \cdot \delta(g), \\ c(f+g) &= c(f) \cdot c(g) \cdot (\delta(f), \delta(g))_p. \end{aligned}$$

Proof. Only the last assertion is not completely obvious. Suppose the forms are in diagonal form $\alpha_1 X_1^2+\cdots+\alpha_m X_m^2$ and $\beta_1 Y_1^2+\cdots+\beta_n Y_n^2$. Then

$$c(f+g)=\prod_{1\le i<j\le m}(\alpha_i,\alpha_j)_p\cdot\prod_{1\le i<j\le n}(\beta_i,\beta_j)_p\cdot\prod_{\substack{1\le i\le m\\1\le j\le n}}(\alpha_i,\beta_j)_p=c(f)\cdot c(g)\cdot(\delta(f),\delta(g))_p.$$

■

Now we go back to theorem 11.2. We assume that p is a finite prime.

1. *Let ϕ be a binary regular quadratic form. ϕ is isotropic iff $\delta(\phi)=-1$ in $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$.*

   We have seen this in lemma 11.3.

2. *Let ϕ be a ternary regular quadratic form. ϕ is isotropic iff $c(\phi)=(-1,-\delta(\phi))_p$.*

   We may assume that $\phi=\alpha_1 X_1^2+\alpha_2 X_2^2+\alpha_3 X^3$. Now it is isotropic iff $\frac{\alpha_1}{-\alpha_3}X_1^2+\frac{\alpha_2}{-\alpha_3}X_2^2-X_3^2$ is isotropic. The corresponding Hilbert symbol is $\left(\frac{\alpha_1}{-\alpha_3},\frac{\alpha_2}{-\alpha_3}\right)_p$, and the Hasse invariant is

   $$c(\phi)=\left(\frac{\alpha_1}{-\alpha_3},\frac{\alpha_2}{-\alpha_3}\right)_p\cdot\underbrace{\left(\frac{\alpha_1}{-\alpha_3},-1\right)_p\cdot\left(\frac{\alpha_2}{-\alpha_3},-1\right)_p}=\left(\frac{\alpha_1}{-\alpha_3},\frac{\alpha_2}{-\alpha_3}\right)_p\cdot(-\delta(\phi),-1)_p.$$

3. *Let ϕ be a quaternary regular form. ϕ is anisotropic iff $c(\phi)=-(-1,-1)_p$ and $\delta(\phi)\in(\mathbb{Q}_p^\times)^2$.*

   We use the following nice trick: write $\phi=f(X_1,X_2)-g(Y_1,Y_2)$ for two binary forms $f(X_1,X_2):=\alpha_1 X_1^2+\alpha_2 X_2^2$ and $g(Y_1,Y_2):=\beta_1 Y_1^2+\beta_2 Y_2^2$.

   We want ϕ to be anisotropic, so this amounts to asking that f and g are both anisotropic, and they do not represent simultaneously some $\gamma\in\mathbb{Q}_p^\times$. By the previous points, this amounts to requiring that

   - $-\alpha_1\alpha_2\notin(\mathbb{Q}_p^\times)^2$ and $-\beta_1\beta_2\notin(\mathbb{Q}_p^\times)^2$ (lemma 11.3).
   - There is no $\gamma\in\mathbb{Q}_p^\times$ such that both

   $$c(f)=(\alpha_1,\alpha_2)_p=(\gamma,-\alpha_1\alpha_2)_p, \tag{*}$$
   $$c(g)=(\beta_1,\beta_2)_p=(\gamma,-\beta_1\beta_2)_p. \tag{**}$$

     are satisfied (lemma 11.4).

   Since $-\alpha_1\alpha_2$ and $-\beta_1\beta_2$ are nonsquares, the symbols $(\gamma,-\alpha_1\alpha_2)_p$ and $(\gamma,-\beta_1\beta_2)_p$ are not identically 1 as functions of γ. Precisely, for half of the classes of $\gamma\in\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ each symbol gives $+1$, and for the other half it gives -1. Thus these halves must be disjoint for (*) and (**). This is equivalent to

   $$\alpha_1\alpha_2=\beta_1\beta_2\pmod{(\mathbb{Q}_p^\times)^2},$$
   $$(\alpha_1,\alpha_2)_p=-(\beta_1,\beta_2)_p.$$

   These two conditions can be written as

   $$\delta(\phi)=\alpha_1\alpha_2\beta_1\beta_2\in(\mathbb{Q}_p^\times)^2,$$
   $$c(\phi)=-(-1,-1)_p.$$

The second identity is derived from multiplicativity of the Hilbert symbol:

$$\begin{aligned} c(\phi) &= (\alpha_1,\alpha_2)_p \cdot (-\beta_1,-\beta_2)_p \cdot \underbrace{(\alpha_1\alpha_2,\beta_1\beta_2)_p}_{=(\beta_1\beta_2,\beta_1\beta_2)_p} \\ &= \underbrace{(\alpha_1,\alpha_2)_p \cdot (\beta_1,\beta_2)_p}_{-1} \cdot (\beta_1,-1)_p \cdot (-1,-\beta_2)_p \cdot (\beta_1\beta_2,\beta_1\beta_2)_p \\ &= -(-1,-\beta_1\beta_2)_p \cdot (\beta_1\beta_2,\beta_1\beta_2)_p \\ &= -(-1,\beta_1\beta_2)_p \cdot (-1,-1)_p \cdot (\beta_1\beta_2,\beta_1\beta_2)_p \\ &= -(-\beta_1\beta_2,\beta_1\beta_2)_p \cdot (-1,-1)_p = -(-1,-1)_p. \end{aligned}$$

Corollary 11.6. *A regular ternary form represents all classes in $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$, except for perhaps one.*

Proof. Let $\phi(X_1,X_2,X_3)$ be a ternary form. It does not represent some $\alpha \in \mathbb{Q}_p^\times$ iff $\phi(X_1,X_2,X_3) - \alpha Y^2$ is anisotropic. The latter requires that $\delta(\phi - \alpha Y^2) = -\alpha\,\delta(\phi)$ is a square. So the only class in $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ that is probably not represented is the inverse of $-\delta(\phi)$. ■

4. *If $n \geq 5$, then a regular quadratic form $\phi(X_1,\ldots,X_n)$ is always isotropic.*

   It is enough to consider the case $n = 5$. Write $\phi = f(X_1,X_2,X_3) - g(Y_1,Y_2)$ where $f(X_1,X_2,X_3)$ is a ternary form and $g(Y_1,Y_2)$ is a binary form. We know from the last corollary that f represents all classes modulo squares, except for perhaps one. $g = \gamma(Y_1^2 - \alpha Y_2^2)$ represents at least half of the classes. If $p < \infty$, then there are at most four classes in $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$, so there must be some β which is represented by both f and g.

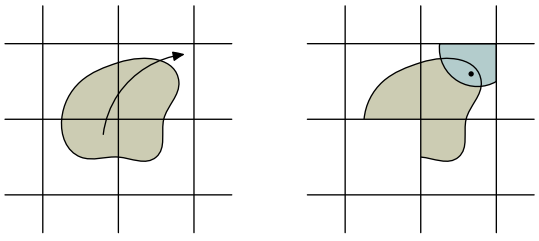
12 Geometry of numbers

Proposition 12.1 (Blichfeld's lemma)**.** *Let $S \subset \mathbb{R}^n$ be a set of Lebesgue measure $\mu(S) > 1$. Then there exist two distinct points $\underline{x}, \underline{y} \in S$ such that $\underline{x} \equiv \underline{y} \pmod{\mathbb{Z}^n}$.*

Proof. Consider the "reduction modulo $\mathbb{Z}^n$". Namely, for each point $\underline{x} \in \mathbb{R}^n$ denote by $\lfloor \underline{x} \rfloor \in \mathbb{Z}^n$ its integral part $(\lfloor x_1 \rfloor, \lfloor x_2 \rfloor, \ldots, \lfloor x_n \rfloor)$. Then define a reduction map by

$$\begin{aligned} f\colon S &\to [0,1)^n, \\ \underline{x} &\mapsto \underline{x} - \lfloor \underline{x} \rfloor. \end{aligned}$$

Since $\mu(S) > 1$ and $\mu([0,1)^n) = 1$, there exist two points $\underline{x}, \underline{y} \in S$ such that $f(\underline{x}) = f(\underline{y})$. ■



Definition 12.2. A subset $S \subseteq \mathbb{R}^n$ is called **convex** if for each two points $\underline{x}, \underline{y} \in S$ the interval between $\underline{x}$ and $\underline{y}$ lies in S, that is

$$(1-t)\,\underline{x} + t\,\underline{y} \in S \quad \text{for all } t \in [0,1].$$

S is **symmetric** if for each point $\underline{x} \in S$ also $-\underline{x} \in S$.

Theorem 12.3 (Minkowski)**.** *Let $S \subseteq \mathbb{R}^n$ be a convex symmetric set of Lebesgue measure $\mu(S) > 2^n$. Then there exists a nonzero integral point $\underline{x} \in S \cap \mathbb{Z}^n$.*

Proof. Consider the set $\frac{1}{2}S$. We have

$$\mu(T) = \frac{1}{2^n}\mu(S) > 1.$$

By Blichfeld's lemma, there exist two distinct points $\underline{y}, \underline{z} \in T$ such that $\underline{y} \equiv \underline{z} \pmod{\mathbb{Z}^n}$. So $\underline{y} - \underline{z} = \underline{x}$ for some $\underline{x} \in \mathbb{Z}^n \setminus \{\underline{0}\}$. We claim that $\underline{x} \in S$.

Since $\underline{y} \in \frac{1}{2}S$, there exists $\underline{y'} \in S$ such that $\underline{y} = \frac{1}{2}\underline{y'}$. Similarly, also taking into account that S is symmetric, $-\underline{z} = \frac{1}{2}\underline{z'}$ for some $\underline{z'} \in S$. By convexity

$$\underline{x} = \frac{1}{2}\underline{y'} + \frac{1}{2}\underline{z'} \in S.$$

■

In the theorem above 2^n cannot be improved. To see this one can just take $S = (-1,1)^n$, which has $\underline{0}$ as the only integral point and $\mu(S) = 2^n$.

If S is assumed to be closed, then a nonstrict inequality $\geq 2^n$ is sufficient. For this consider the sets $S_\epsilon := (1-\epsilon)\,S$. We have $\mu(S_\epsilon) = (1+\epsilon)^n\,\mu(S) > 2^n$. Now for each $\epsilon > 0$ there exists $\underline{x}_\epsilon \neq \underline{0}$ such that $\underline{x}_\epsilon \in S_\epsilon \cap \mathbb{Z}^n$. Among such $\underline{x}_\epsilon$ there is $\underline{x} \neq \underline{0}$ that belongs to all S_ϵ, and so $\underline{x} \in \bigcap_{\epsilon>0} S_\epsilon$, and the latter intersection is S, by assumed compactness.

Now we will derive some corollaries from the Minkowski theorem.

Corollary 12.4. *Let $L_1, \ldots, L_n$ be a system of linear forms on $\mathbb{R}^n$. Let $c_1, \ldots, c_n \in \mathbb{R}_{>0}$. Assume that $|\det(L_1, \ldots, L_n)| < c_1 \cdots c_n$. Then there exists a nonzero integral point $\underline{x} \in \mathbb{Z}^n \setminus \{\underline{0}\}$ such that $|L_i(\underline{x})| < c_i$ for $i = 1, \ldots, n$.*

Proof. We apply the Minkowski theorem to a convex set

$$S := \{\underline{x} \in \mathbb{R}^n \mid |L_i(\underline{x})| < c_i,\ 1 \leq i \leq n\}.$$

The result is immediate after we compute the volume:

$$\mu(S) = 2^n \frac{c_1 \cdots c_n}{|\det(L_1, \ldots, L_n)|}.$$

■

If in the statement above we replace $|L_i(\underline{x})| < c_i$ with $|L_i(\underline{x})| \leq c_i$, then $|\det(L_1, \ldots, L_n)| < c_1 \cdots c_n$ can be also replaced with $|\det(L_1, \ldots, L_n)| \leq c_1 \cdots c_n$. In fact, it is sufficient to have only $|L_1(\underline{x})| \leq c_1$ and $|L_i(\underline{x})| < c_i$ for $i = 2, \ldots, n$.

Corollary 12.5 (Dirichlet approximation theorem)**.** *Let $\alpha \in \mathbb{R}$ and let $Q > 0$. Then there exist $x, y \in \mathbb{Z}$, $(x, y) \neq (0, 0)$, such that $|x\alpha - y| < Q^{-1}$ and $|x| \leq Q$.*

Sometimes this statement is written in form

$$\left|\alpha - \frac{y}{x}\right| < \frac{1}{Qx} \leq \frac{1}{x^2}.$$

This means that one can approximate a real number with a rational fraction $\frac{y}{x}$ with precision $\frac{1}{x^2}$.

Proof of the corollary. Consider linear forms $L_1(x, y) = \alpha x - y$ and $L_2(x, y) = x$. Apply the previous corollary for $c_1 = Q^{-1}$ and $c_2 = Q$. ■

One can show that there exist infinitely many rational numbers $\frac{y}{x} \in \mathbb{Q}$ such that

$$\left|\alpha - \frac{y}{x}\right| < \frac{1}{x^2}.$$

(Such approximations come from continuous fraction expansions.)

Proposition 12.6. *Let $L_1, \dots, L_s$ be linear forms on $\mathbb{Z}^n$ with coefficients in $\mathbb{Z}$. Let $m_1, \dots, m_s \in \mathbb{Z}_{>0}$. Let S be a symmetric convex set in $\mathbb{R}^n$. Assume $\mu(S) > 2^n m_1 \cdots m_s$. Then there exists $\underline{x} \in \mathbb{Z}^n \cap S$, $\underline{x} \neq \underline{0}$, such that*

$$L_i(\underline{x}) \equiv 0 \pmod{m_i} \quad i = 1, \dots, s. \tag{*}$$

Proof. Consider

$$\Lambda := \{\underline{x} \in \mathbb{Z}^n \mid \underline{x} \text{ satisfies (*)}\}.$$

It is a subgroup of $\mathbb{Z}^n$ of index m.

We want to apply a generalized Blichfeld's theorem (the proof goes the same way, so we omit it).

Claim. *Let $S \subseteq \mathbb{R}^n$ be a symmetric convex set. Let $m \in \mathbb{Z}_{>0}$. If $\mu(S) > m$, then there exist $m+1$ pairwise distinct points $\underline{y}_0, \dots, \underline{y}_m \in S$ such that $\underline{y}_i - \underline{y}_j \in \mathbb{Z}^n$.*

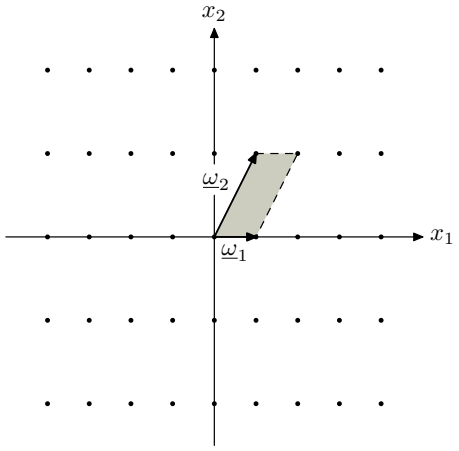
We have $\mu(\frac{1}{2}S) > m$ for $m := m_1 \cdots m_s$, so in our case there are pairwise distinct points $\underline{y}_0, \dots, \underline{y}_m \in \frac{1}{2}S$ such that $\underline{y}_i - \underline{y}_j \in \mathbb{Z}^n$. Among them there must be a pair $\underline{y}_i, \underline{y}_j$ such that $\underline{y}_i \equiv \underline{y}_j \pmod{\Lambda}$, i.e. $\underline{y}_i - \underline{y}_j \in \Lambda$. ■

In the proof above Λ is a **lattice**, that is a discrete subgroup of rank n in $\mathbb{R}^n$. A lattice has form

$$\Lambda = \{x_1\underline{\omega}_1 + \cdots + x_n\underline{\omega}_n \mid x_i \in \mathbb{Z}\},$$

where $\underline{\omega}_1, \dots, \underline{\omega}_n \in \mathbb{Z}^n$ are linearly independent over $\mathbb{R}$.

The **determinant** of Λ is the volume of its fundamental parallelepiped. It coincides with the subgroup index $[\mathbb{Z}^n : \Lambda]$.



One can formulate the Minkowski theorem for arbitrary lattices.

Proposition 12.7 (Minkowski revised)**.** *Let S be a symmetric convex set in $\mathbb{R}^n$ and let $\Lambda \subset \mathbb{R}^n$ be a lattice. If $\mu(S) > 2^n \det\Lambda$, then $S \cap \Lambda$ has a nonzero point.*

(This easily reduces to the usual case $\Lambda = \mathbb{Z}^n$ by a variable change.)

13 Proof of the Hasse–Minkowski theorem

With the developed tools we can finally prove the Hasse–Minkowski theorem. It can be reformulated as follows in our new language. *Let $\phi(\underline{X})$ be a quadratic form over $\mathbb{Q}$. Then*

$$\phi \text{ is isotropic over } \mathbb{Q} \iff \phi \text{ is isotropic over } \mathbb{Q}_p \text{ for } 2 \le p \le \infty.$$

Let n denote the dimension (the number of variables $X_1, \dots, X_n$).

For $n = 1$ there is nothing to prove—the form is not isotropic. ■

For $n = 2$, replacing ϕ with $\alpha\phi$ for some $\alpha \in \mathbb{Q}^\times$, we may assume $\phi(X, Y) = X^2 - \alpha Y^2$. Now $X^2 - \alpha Y^2$ is isotropic over K iff α is a square in K. So we have to show

$$\alpha \in (\mathbb{Q}^\times)^2 \iff \alpha \in (\mathbb{Q}_p^\times)^2 \text{ for } 2 \le p \le \infty.$$

In one direction this is obvious. In the other direction, suppose $\alpha \in (\mathbb{Q}_p^\times)^2$ for every prime p. Write $\alpha = \epsilon \prod p^{v_p(\alpha)}$ for $\epsilon = \pm 1$. Since $\alpha \in (\mathbb{R}^\times)^2$, we have $\epsilon = +1$. Now since $\alpha \in (\mathbb{Q}_p^\times)^2$ for finite p, each $v_p(\alpha)$ is even. Thus $\alpha \in (\mathbb{Q}^\times)^2$. ■

Ternary forms case

Things become really interesting starting from $n = 3$. The study of this particular case (but of course not our proof with quadratic forms and geometry of numbers) can be attributed to Legendre.

We may assume that the quadratic form is regular and has form

$$\phi(X_1, X_2, X_3) = a_1 X_1^2 + a_2 X_2^2 + a_3 X_3^2$$

with $a_i \in \mathbb{Z}$, $a_i \neq 0$, and $a_1\, a_2\, a_3$ square-free (if $p^2 \mid a_i$ for some prime p, this can be ruled out by a variable change $X_i' := p X_i$). We claim one can even assume that $a_1, a_2, a_3 \in \mathbb{Z}$ with a_1, a_2, a_3 being *pairwise* coprime.

Assume p divides both a_1 and a_2. Consider a quadratic form

$$p\phi \sim \frac{a_1}{p} X_1^2 + \frac{a_2}{p} X_2^2 + p\, a_3\, X_3^2.$$

Now the coefficients are $a_1' = a_1/p$, $a_2' = a_2/p$, $a_3' = p\, a_3$. We have $|a_1'\, a_2'\, a_3'| = \frac{|a_1\, a_2\, a_3|}{p}$, so after finitely many steps like that we obtain $(a_i, a_j) = 1$ for $i \neq j$.

It is clear that if ϕ is isotropic over $\mathbb{Q}$, then it is isotropic over $\mathbb{Q}_p$. We want to show the opposite implication. Assume ϕ is isotropic over $\mathbb{Q}_p$ for all p.

We look what does it mean that ϕ is isotropic over $\mathbb{Q}_p$ with $p < \infty$? If $p \neq 2$ and all a_i are units, that is $p \nmid a_1\, a_2\, a_3$, then ϕ is automatically isotropic over $\mathbb{Q}_p$ (proposition 9.1). We look at what happens when $p \mid a_1\, a_2\, a_3$ or $p = 2$.

Suppose $p > 2$ and $p \mid a_1\, a_2\, a_3$. We may assume that $p \mid a_3$. The form ϕ is isotropic if there exist $x_1, x_2, x_3 \in \mathbb{Q}_p$, $(x_1, x_2, x_3) \neq (0, 0, 0)$, such that $a_1 x_1^2 + a_2 x_2^2 + a_3 x_3^2 = 0$. We can clearly assume that one of x_i's is a unit. Actually, it must be the case that at least two x_i's are units, so that at least one of $v_p(x_1)$ and $v_p(x_2)$ is zero. If not, then $v_p(x_1) \ge 1$, $v_p(x_2) \ge 1$, $v_p(x_3) = 0$, and

$$v_p(a_1 x_1^2 + a_2 x_2^2) \ge 2, \quad v_p(a_3 x_3^2) = 1,$$

contradicting $v_p(a_1 x_1^2 + a_2 x_2^2) = v_p(a_3 x_3^2)$.

Now reducing modulo p, we get from our assumptions that $a_1 X_1^2 + a_2 X_2^2$ is isotropic over $\mathbb{F}_p$, and so $a_1(X_1^2 - b X_2^2)$ is isotropic for $b := a_2\, a_1^{-1}$, meaning that $b = c^2$ is a square. So we get

$$\phi \equiv a_1 (X_1^2 - b X_2^2) = L_1(X_1, X_2) \cdot L_2(X_1, X_2) \pmod{p}, \quad L_1 := a_1(X_1 - c X_2),\ L_2 := X_1 + c X_2.$$

Thus far we have deduced the following: *if ϕ is isotropic over $\mathbb{Q}_p$ for $p \mid a_1\,a_2\,a_3$, $p>2$, then there exist linear forms $L_1^{(p)}, L_2^{(p)} \in \mathbb{Z}[\underline{X}]$ such that $\phi \equiv L_1^{(p)} \cdot L_2^{(p)} \pmod p$.* (These forms depend on p, as we have seen above.)

Next we analyze the case $p=2$ (see p. 28). If $2 \nmid a_1\,a_2\,a_3$, then

$$\phi \text{ is isotropic over } \mathbb{Q}_2 \iff a_i + a_j \equiv 0 \pmod 4 \text{ for some } i \neq j.$$

If $2 \mid a_1\,a_2\,a_3$, e.g. $2 \mid a_3$, then

$$\phi \text{ is isotropic over } \mathbb{Q}_2 \iff \left\{ \begin{array}{c} a_1 + a_2 \equiv 0 \pmod 8 \\ \text{or} \\ a_1 + a_2 + a_3 \equiv 0 \pmod 8 \end{array} \right\}$$

- For every odd prime $p \mid a_1\,a_2\,a_3$ we consider congruences

$$L_1^{(p)}(\underline{X}) \equiv 0 \pmod p \quad \text{or} \quad L_2^{(p)}(\underline{X}) \equiv 0 \pmod p.$$

- If $2 \nmid a_1\,a_2\,a_3$ and, say, $a_1 + a_2 \equiv 0 \pmod 4$, consider congruences

$$X_1 \equiv X_2 \pmod 2, \quad X_3 \equiv 0 \pmod 2.$$

- If $2 \mid a_1\,a_2\,a_3$, e.g. $2 \mid a_3$, consider congruences

$$X_1 \equiv X_2 \pmod 4,$$

$$X_3 \equiv \left\{ \begin{array}{ll} 0 \pmod 2, & \text{if } a_1 + a_2 \equiv 0 \pmod 8, \\ X_2 \pmod 2, & \text{if } a_1 + a_2 + a_3 \equiv 0 \pmod 8. \end{array} \right.$$

Totally we have a linear congruence modulo p for each odd $p \mid a_1\,a_2\,a_3$. For $p=2$ and $2 \nmid a_1\,a_2\,a_3$ we have two congruences modulo 2; for $p=2$ and $2 \mid a_1\,a_2\,a_3$ we have one congruence modulo 4 and two congruences modulo 2. In any case, the product of moduli is

$$\Big(\prod_{\substack{p>2 \\ p \mid a_1\,a_2\,a_3}} p \Big) \cdot \left\{ \begin{array}{ll} 2 \cdot 2, & \text{if } 2 \nmid a_1\,a_2\,a_3, \\ 2 \cdot 4, & \text{if } 2 \mid a_1\,a_2\,a_3. \end{array} \right\} = 4 \cdot |a_1\,a_2\,a_3|.$$

If p is odd, then the congruence $L_i^{(p)}(\underline{X}) \equiv 0 \pmod p$ implies $\phi(\underline{X}) \equiv 0 \pmod p$.
If $a_1 + a_2 \equiv 0 \pmod 4$ and $X_1 \equiv X_2 \pmod 2$, $X_3 \equiv 0 \pmod 2$, then

$$\phi(\underline{X}) \equiv a_1 X_1^2 + a_2 X_2^2 \equiv 0 \pmod 4$$

Similarly, if $2 \mid a_1\,a_2\,a_3$, then the congruences give $\phi(\underline{X}) = 0 \pmod 8$.
So our congruences mean that

$$\begin{aligned} &\phi(\underline{X}) \equiv 0 \pmod p \quad \text{for } p>2,\ p \mid a_1\,a_2\,a_3, \\ &\phi(\underline{X}) \equiv 0 \pmod 4 \quad \text{for } 2 \nmid a_1\,a_2\,a_3, \\ &\phi(\underline{X}) \equiv 0 \pmod 8 \quad \text{for } 2 \mid a_1\,a_2\,a_3, \end{aligned}$$

which implies $\phi(\underline{X}) \equiv 0 \pmod{4 \cdot |a_1\,a_2\,a_3|}$. However, we gave this condition by *linear* congruences, and not quadratic. This means that we can apply corollary 12.4.

Consider a convex set

$$S := \{\underline{x} \in \mathbb{R} \mid |a_1| \cdot x_1^2 + |a_2| \cdot x_2^2 + |a_3| \cdot x_3^2 < 4 \cdot |a_1\, a_2\, a_3|\}.$$

It is an ellipsoid, having volume

$$\mu(S) = \frac{\frac{3}{4}\pi(\sqrt{4 \cdot |a_1\, a_2\, a_3|})^3}{\sqrt{|a_1|}\,\sqrt{|a_2|}\,\sqrt{|a_3|}} = 8 \cdot \frac{4}{3}\pi \cdot |a_1\, a_2\, a_3| > 2^3 \cdot \underbrace{4 \cdot |a_1\, a_2\, a_3|}_{m \text{ in corollary 12.4}}.$$

So S should have an integral point satisfying all the congruences. There is $\underline{x}$ such that $\phi(\underline{x}) \equiv 0 \pmod{4 \cdot |a_1\, a_2\, a_3|}$. But since $\underline{x} \in S$, that implies $\phi(\underline{x}) = 0$, and ϕ is isotropic over $\mathbb{Q}$. ■

Observe that in our argument we actually did not use the condition that ϕ is isotropic over $\mathbb{Q}_\infty = \mathbb{R}$. There is no contradiction because, as we saw in corollary 10.6, there is always an even number of p's such that a given ternary quadratic form is anisotropic over $\mathbb{Q}_p$. So disregarding one prime (in our proof $p = \infty$) does not affect the result.

Corollary 13.1. *Let f be a regular binary form. Let $a \in \mathbb{Q}^\times$. Then f represents a over $\mathbb{Q}$ iff f represents a over $\mathbb{Q}_p$ for all primes $2 \le p \le \infty$.*

Proof. Consider a ternary form $f(X,Y) - a\,Z^2$. It is isotropic iff f represents a. ■

Quaternary forms case

We will need the following famous result about primes in arithmetic progressions:

Theorem 13.2 (Dirichlet)**.** *Let $m \in \mathbb{Z}$ be a nonzero integer and let $a \in \mathbb{Z}$ be such that $(m,a) = 1$. Then there are infinitely many primes q such that $q \equiv a \pmod{m}$*

For a proof see any textbook in analytic number theory.

Example 13.3. There are infinitely many primes q such that $q \equiv 1 \pmod 3$, or $q \equiv 3 \pmod 4$, etc. ▲

We proceed with the Hasse–Minkowski theorem for quaternary quadratic forms. Consider a quadratic form $f = a_1 X_1^2 + a_2 X_2^2 + a_3 X_3^2 + a_4 X_4^2$ with $a_i \in \mathbb{Q}^\times$. We want to show that if f is isotropic over $\mathbb{Q}_p$ for all $2 \le p \le \infty$, then f is isotropic over $\mathbb{Q}$.

We may assume that $a_i \in \mathbb{Z}$ are squarefree integers. Since f is isotropic over $\mathbb{R}$, the coefficients are not of the same sign. We may assume $a_1 > 0$ and $a_4 < 0$. Write the quadratic form as $f = g(X_1, X_2) - h(X_3, X_4)$, where $g := a_1 X_1^2 + a_2 X_2^2$ and $h := -a_3 X_3^2 - a_4 X_4^2$. Consider the set of prime divisors of a_i, together with 2 (which is always a "bad prime" to be treated separately):

$$S := \{p \mid p \mid a_1\, a_2\, a_3\, a_4\} \cup \{2\}.$$

Now if for $p \in S$ the form f is isotropic over $\mathbb{Q}_p$, then there exists some $b_p \in \mathbb{Q}_p^\times$ represented by both g and h (proposition 8.21). We may assume $v_p(b_p) = 0$ or 1.

Now there exists $b \in \mathbb{Z}$ such that

$$\begin{aligned} b &\equiv b_p \pmod{p^2} \quad \text{for } p \in S, p \neq 2, \\ b &\equiv b_2 \pmod{16}. \end{aligned}$$

So $b\,b_p^{-1} \equiv 1 \pmod p$ for $p \in S$, $p \neq 2$ and $b\,b_2 \equiv 1 \pmod 8$. Now $b\,b_p \in (\mathbb{Q}_p^\times)^2$, so b itself is represented by g and h over $\mathbb{Q}_p$, $p \in S$.

We may assume $b > 0$. Then b is represented by g and h over $\mathbb{R}$ (because $a_1 > 0$, $-a_4 > 0$).

Assume q is an odd prime such that $q \notin S$, $q \nmid b$. Then b is represented by g and by h over $\mathbb{Q}_q$, because the coefficients of $g(X_1, X_2) - b\,Y^2$, $h(X_3, X_4) - b\,Y^2$ are q-adic units.

What if $q \notin S$ and $q \mid b$? We claim that there is at most one such prime.

Claim. *b satisfying the congruences $b \equiv b_p \pmod{p^2}$ and $b \equiv b_2 \pmod{16}$ above can be chosen to have at most one prime divisor $q \notin S$.*

Assuming this claim, we have that b is represented over $\mathbb{Q}_p$ for all primes $2 \le p \le \infty$ by both g and h, except for perhaps one prime. This means that b is represented over $\mathbb{Q}$, and so $f = g - h$ is isotropic over $\mathbb{Q}$.

It remains to show the claim above.

Proof. Consider the set

$$S' := \{p \in S \mid p \mid b_p\}.$$

Then we have

$$b = \left(\prod_{p \in S'} p\right) \cdot b', \quad (b', p) = 1 \text{ for all } p \in S.$$

Consider an integer

$$m := \frac{16 \cdot \prod_{p \in S} p^2}{\prod_{p \in S'} p}.$$

Now the congruences above are equivalent to $b' \equiv c \pmod{m}$ for some $c \in \mathbb{Z}$, where $(c, m) = 1$. By Dirichlet's theorem, we can take a prime $b' = q$. ■

Forms of dimension ≥ 5

Consider a quadratic form in five variables $f = a_1 X_1^2 + \cdots + a_5 X_5^2$ with $a_i \in \mathbb{Z}$, which is isotropic over $\mathbb{Q}_p$ for all p. We can assume that a_i are square-free, and, say, $a_1 > 0$ and $a_5 < 0$ (since the form is isotropic over $\mathbb{R}$).

We have $f = g(X_1, X_2) - h(X_3, X_4, X_5)$ for $g := a_1 X_1^2 + a_2 X_2^2$ and $h := -a_3 X_3^2 - a_4 X_4^2 - a_5 X_5^2$. Consider the set

$$S := \{p \mid p \mid a_1 a_2 a_3 a_4 a_5\} \cup \{2\}.$$

There exists $b \in \mathbb{Z}$, $b \neq 0$, represented by both g and h over $\mathbb{Q}_p$ for all $p \in S$, $p \nmid b$ and also for $p = \infty$. Again, by Dirichlet's theorem, we may assume that b has at most one prime divisor $q \notin S$.

Since $q \nmid a_3 a_4 a_5$, we have that h is isotropic over $\mathbb{Q}_q$, and g represents b over $\mathbb{Q}_q$.

Now b is represented over $\mathbb{Q}_p$ by both g and h for all primes $2 \le p \le \infty$, so b is represented over $\mathbb{Q}$ by both g and h, meaning that $f = g - h$ is isotropic over $\mathbb{Q}$. ■

For $n > 5$ one proceeds by induction. Consider a form $f = a_1 X_1^2 + \cdots + a_n X_n^2$. Assume it is isotropic over $\mathbb{Q}_p$ for all $2 \le p \le \infty$. In particular, it is isotropic over $\mathbb{R}$, hence we can consider $f = g + h$, where g is a form in 5 variables isotropic over $\mathbb{R}$ (we choose g such that not all its coefficients have the same sign). By the Hasse–Minkowski principle for $n = 5$ we have that g is isotropic over $\mathbb{Q}$, and we are done by induction. ■

Part II
Intermezzo: more on absolute values

14 Extensions of complete fields

Let K be a field complete with respect to an absolute value $|\cdot|$. Let L be a finite extension of K. Then

- it is possible to extend $|\cdot|$ to L,
- such extension is unique,
- L will be also complete with respect to the extended absolute value.

The extension of an absolute value $|\cdot|$ to L is given by

$$\begin{aligned} L &\to \mathbb{R}_{\geq 0}, \\ \alpha &\mapsto |N_{L/K}(\alpha)|^{1/n}. \end{aligned}$$

Here $N_{L/K}$ is the norm map of the extension L/K and $n = [L : K]$ is the extension degree.

As a corollary, an absolute value extends uniquely to the algebraic closure $\overline{K}$, but one should be careful because it is not complete anymore. One can take completion of $\overline{K}$, and it will be an algebraically closed field.

Theorem 14.1. *Completion of an algebraically closed field is algebraically closed.*

For archimedian fields the situation is simple, because of the following result, named after Israel Gelfand and Stanisław Mazur.

Theorem 14.2 (Gelfand–Mazur)**.** *The only archimedian complete fields are* $\mathbb{R}$ *and* $\mathbb{C}$.

So we will focus on the nonarchimedian complete fields.

Example 14.3. There are two principally different situations.

The "equal characteristic case" means that F_K and K have the same characteristic. The basic example is $K = F((T))$, $O_K = F[[T]]$, $F_K = F$.

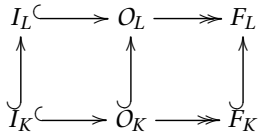
The "distinct characteristic case" means that F_K has characteristic > 0 and K has characteristic 0. The basic example of this is $K = \mathbb{Q}_p$, $O_K = \mathbb{Z}_p$, $F_K = \mathbb{F}_p$. ▲

We fix the following notation:

- K is a nonarchimedian complete field with respect to an absolute value $|\cdot|$.
- $O_K := \{\alpha \in K \mid |\alpha| \leq 1\}$ is the **local ring** of K.
- $I_K := \{\alpha \in K \mid |\alpha| < 1\}$ is the maximal ideal in O_K.
- $F_K := O_K / I_K$ is the **residue field** of K.
- $\Gamma_K := \{|\alpha| \mid \alpha \in K^\times\}$ is a multiplicative subgroup of $\mathbb{R}_{>0}$.

An important case is that of **discrete absolute values**, when Γ_K is a discrete subgroup, as it happens for $\mathbb{Q}_p$ and $F((T))$. In this case it is convenient to consider not the absolute value $|\cdot|_v$ but the corresponding discrete valuation $v(\cdot)$. In such situation we pass from a multiplicative group to an additive group that normalizes to be $\mathbb{Z}$.

Let K be a complete field and let L/K be a finite extension. We have



$$I_K = O_K \cap I_L.$$

The image of O_K under the quotient map $O_L \to F_L$ is the residue field F_K.

Proposition 14.4. *F_L/F_K is a finite field extension and $[F_L : F_K] \le [L : K]$.*

Proof. Let $\overline{\alpha}_1, \dots, \overline{\alpha}_n \in F_L$ be linearly independent over F_K. We claim that the lifts $\alpha_1, \dots, \alpha_n \in O_L$ are linearly independent over K.

Assume $\lambda_1\alpha_1 + \dots + \lambda_n\alpha_n = 0$ for some $\lambda_1, \dots, \lambda_n \in K$ and $(\lambda_1, \dots, \lambda_n) \neq (0, \dots, 0)$. We may assume (multiplying the identity by some number) that $|\lambda_i| \le 1$ and for some i we have $|\lambda_i| = 1$. Then $\lambda_i \in O_L$ and in F_K holds $\overline{\lambda}_1\overline{\alpha}_1 + \dots + \overline{\lambda}_n\overline{\alpha}_n = 0$ for $(\overline{\lambda}_1, \dots, \overline{\lambda}_n) \neq (0, \dots, 0)$. Contradiction. ■

For an extension L/K the group Γ_K is a subgroup of Γ_L.

Proposition 14.5. $[\Gamma_L : \Gamma_K] \le [L : K]$.

Proof. Consider $\alpha_1, \dots, \alpha_n \in L^\times$ such that $|\alpha_1|, \dots, |\alpha_n|$ represent pairwise distinct cosets of Γ_L/Γ_K. We claim that $\alpha_1, \dots, \alpha_n$ are linearly independent over K.

Assume for the sake of contradiction that $\lambda_1\alpha_1 + \dots + \lambda_n\alpha_n = 0$ for some $(\lambda_1, \dots, \lambda_n) \neq (0, \dots, 0)$. We may assume that $\lambda_1, \dots, \lambda_n \neq 0$ (by throwing away zero terms). Now each $|\lambda_i\alpha_i|$ belongs to the same coset in Γ_L/Γ_K as $|\alpha_i|$, so all $|\lambda_i\alpha_i|$ represent pairwise distinct cosets. Hence $\lambda_1\alpha_1 + \dots + \lambda_n\alpha_n \neq 0$, since in the nonarchimedian setting $a_1 + \dots + a_n = 0$ implies $|a_i| = |a_j|$ for some $i \neq j$. Contradiction. ■

Definition 14.6. Let L/K be a finite extension of complete local fields.

The number $f_{L/K} := [F_L : F_K]$ is called the **residue field degree** of the extension.

The number $e_{L/K} := [\Gamma_L : \Gamma_K]$ is called the **ramification index**.

In case of discrete absolute values the group Γ_K is discrete. We have $\Gamma_K = \langle |\pi_K| \rangle$ where π_K is the primitive element generating the maximal ideal $I_K \subset O_K$.

Example 14.7. For $\mathbb{Q}_p$ we have $\pi = p$. For $F((T))$ we have $\pi = T$. ▲

Every $\alpha \in K$ can be uniquely written as $\pi^m\eta$ for some unit $\eta \in O_K^\times$. Then we can define a valuation $v_\pi(\alpha) := m$ and the corresponding absolute value $|\alpha| := |\pi|^{-v_\pi(\alpha)}$. This is essentially what we did in § 1 for p-adic integers; the same works for an arbitrary discrete valuation ring.

The ramification index is $e_{L/K} = [|\pi_L|\mathbb{Z} : |\pi_K|\mathbb{Z}]$. We have $|\pi_L|^\ell = |\pi_K|$ and $\pi_K = \pi_L^\ell\eta$ for $\eta \in O_L^\times$.

We have seen that $e_{L/K} \le [L : K]$ and $f_{L/K} \le [L : K]$. In fact, a stronger fact holds

Proposition 14.8. $e_{L/K} \cdot f_{L/K} \le [L : K]$.

In the most interesting cases $e_{L/K} \cdot f_{L/K} = [L : K]$, e.g. in the case when F_L/F_K is a separable extension (for instance, when F_K is a perfect field).

Proof. Let $\alpha_1, \dots, \alpha_e$ be such that $|\alpha_1|, \dots, |\alpha_e|$ represent all residue classes of Γ_L/Γ_K. Let $\overline{\beta}_1, \dots, \overline{\beta}_f \in O_L/I_L$ be a basis of F_L/F_K and $\beta_1, \dots, \beta_f$ are some lifts to O_L.

We have ef elements $\alpha_i\beta_j$ and we claim they are linearly independent over K. Assume it is not the case and

$$\sum_{\substack{1 \le i \le e \\ 1 \le j \le f}} \lambda_{ij}\alpha_i\beta_j = 0$$

for some λ_{ij}, not all equal to 0.

Consider the absolute values $|\lambda_{ij}\,\alpha_i\,\beta_j|$. Let (i_1, j_1) be the index such that $\delta := |\lambda_{i_1,j_1}\,\alpha_{i_1}\,\beta_{j_1}|$ is maximal among all. Consider all other indices giving the same value:

$$S := \{(i,j) \mid |\lambda_{ij}\,\alpha_i\,\beta_j| = \delta\}.$$

Now since $\beta_j \in O_L^\times$, we have $|\beta_j| = 1$, and for all $(i,j) \in S$ the values $|\lambda_{ij}\,\alpha_i|$ are equal. In particular, they belong to the same class Γ_L/Γ_K, meaning that all i's are the same.

We may assume that $|\lambda_{i_1,j}| \le 1$ for all j and $|\lambda_{i_1,j}| = 1$ for some j.

We have $|\lambda_{i_1,j}\,\alpha_{i_1}\,\beta_j| = |\lambda_{i_1,j}| \cdot |\alpha_{i_1}|$.

$$\left|\sum_{(i_1,j)\in S} \lambda_{i_1,j}\,\beta_j\right| < 1.$$

So reducing $\sum_{(i_1,j)\in S} \lambda_{i_1,j}\,\beta_j$ modulo I_K, we get

$$\sum_{(i_1,j)\in S} \overline{\lambda}_{i_1,j}\,\overline{\beta}_j = 0,$$

where not all $\lambda_{i_1,j}$ are 0. Contradiction. ■

15 Discrete absolute values case

Let K be complete with respect to a discrete absolute value $|\cdot|$. We claim that in this case $e_{L/K} \cdot f_{L/K} = [L:K]$.

Lemma 15.1. *Let R be a principal ideal domain. Let M be a free R-module. Then every R-submodule of M is also free.*

(If M is finitely generated, this follows from the structure of finitely generated modules over a PID. For the infinite version see *Lang, Algebra*, Appendix 2, §2, p. 880.)

Lemma 15.2. *Let L/K be an extension of discrete complete local fields. Then O_L is a free O_K-module of rank $[L:K]$.*

Proof. Since $|\cdot|$ is discrete, every ideal of O_K is generated by π_K^m for $m = 0, 1, 2, \ldots$ In particular, O_K is a principal ideal domain, and we are going to use this fact.

Let $\alpha_1, \ldots, \alpha_n$ be a K-basis of L. We may assume that these elements lie in O_L. Consider the O_K-module

$$M := O_K\alpha_1 \oplus \cdots \oplus O_K\alpha_n.$$

It is an O_K-submodule of O_L.

For an element $\alpha = \lambda_1\,\alpha_1 + \cdots + \lambda_n\,\alpha_n \in O_L$ the coefficients $\lambda_i \in K$ are given by the linear system of equations

$$\mathrm{tr}_{L/K}(\alpha_i\,\alpha) = \sum_j \mathrm{tr}_{L/K}(\alpha_i\,\alpha_j)\,\lambda_j.$$

Now $\mathrm{tr}_{L/K}(\alpha_i\,\alpha) \in O_L \cap K = O_K$, so $d\,\lambda_j \in O_K$, where $d = \det[\mathrm{tr}_{L/K}(\alpha_i\,\alpha_j)] \in O_K$ is the determinant of the linear system.

We have $d\,O_L \subseteq M$. Now M is a free O_K-module, and so $d\,O_L$ (since O_K is a principal ideal domain!) and O_L. We must conclude that $O_L = M$ is a free O_K-module of rank $n = [L:K]$. ■

Remark 15.3. Observe that we used above just that O_K is a principal ideal domain. If K and L are number fields, then O_L is also a free O_K-module of rank $[L:K]$, but O_K may not be a PID.

Lemma 15.4. *$O_L/\pi_K O_L$ is a $[L:K]$-dimensional vector space over F_K.*

Proof. We have an isomorphism of O_K-modules $O_L \cong O_K^n$, hence $O_L/\pi_K O_L \cong (O_K/\pi_K O_K)^n \cong F_K^n$. ■

$F_L := O_L / I_L$ is an $f_{L/K}$-dimensional F_K-vector space by the definition of the residue field degree $f_{L/K}$. Moreover, the following is true:

Lemma 15.5. *For each m the quotient $I_L^m / I_L^{m+1} = \pi_L^m O_L / \pi_L^{m+1} O_L$ is an $f_{L/K}$-dimensional F_K-vector space isomorphic to F_L.*

Proof. Consider a homomorphism of O_K-modules

$$O_L \to \frac{\pi_L^m O_L}{\pi_L^{m+1} O_L},$$
$$x \mapsto \pi_L^m \cdot x.$$

This is a surjection and the kernel is $\pi_L O_L$, hence the isomorphism

$$F_L := \frac{O_L}{\pi_L O_L} \cong \frac{\pi_L^m O_L}{\pi_L^{m+1} O_L}.$$

■

Example 15.6. For p-adic integers we have an isomorphism of $\mathbb{F}_p$-vector spaces

$$\frac{p^m \mathbb{Z}_p}{p^{m+1} \mathbb{Z}_p} \cong \frac{\mathbb{Z}_p}{p \mathbb{Z}_p}.$$

▲

Theorem 15.7. *Let L/K be an extension of discrete complete local fields. Then $e_{L/K} \cdot f_{L/K} = [L : K]$.*

Proof. $O_L / \pi_K O_L \cong F_K^n$ where $n := [L : K]$, as an F_K-vector space.

We have $\pi_L^e \equiv \pi_K$ by definition of $e = e_{L/K}$. Consider a filtration

$$\pi_K O_L = \pi_L^e O_L \subseteq \pi_L^{e-1} O_L \subseteq \cdots \subseteq \pi_L O_L \subseteq O_L.$$

Each quotient $\pi_L^m O_L / \pi_L^{m+1} O_L$ is an f-dimensional F_K-vector space, so we have a tower of such vector spaces

$$O_L / \pi_K O_L \geq O_L / \pi_L^{e-1} O_L \geq \cdots \geq O_L / \pi_L O_L \geq \{0\}.$$

There are e vector spaces in this tower, and on each step the dimension increases by f, so

$$\dim_{F_K} O_L / \pi_K O_L = e f.$$

■

Moreover, from the proof we see that if $\overline{\theta}_1, \ldots, \overline{\theta}_f$ is a basis of F_L / F_K, then for some lifts $\theta_1, \ldots, \theta_f$ to O_L, a basis of O_L as an O_K-module is

$$\theta_i \pi_L^j, \quad 1 \leq i \leq f_{L/K},\ 0 \leq j \leq e_{L/K} - 1.$$

Remark 15.8. For local fields there is only one prime $\pi_K \in O_K$ and one prime $\pi_L \in O_L$, so that the factorization into prime ideals in O_L comes down to

$$\pi_K O_L = \langle \pi_L^e \rangle.$$

But for example, if L and K are number fields, then there are many prime ideals $\mathfrak{p} \subset O_K$, and for each one we can consider the unique factorization

$$\mathfrak{p} O_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_s^{e_s} \qquad (*)$$

into prime ideals $\mathfrak{P}_i \subset O_L$. We define for each $\mathfrak{P}_i$ the residue field degree to be $f_i := [O_L/\mathfrak{P}_i : O_K/\mathfrak{p}]$.

Recall that the **norm** $N(\mathfrak{a})$ of an ideal $\mathfrak{a} \subseteq O_L$ is defined to be the ideal $N(\mathfrak{a}) \subseteq O_K$ generated by $N_{K/L}(x)$ for all $x \in \mathfrak{a}$.

- For a prime ideal $\mathfrak{P}_i \subset O_L$ one has $N(\mathfrak{P}_i) = \mathfrak{p}^{f_i}$, where $\mathfrak{p} = O_K \cap \mathfrak{P}_i$ and $f_i := [O_L/\mathfrak{P}_i : O_K/\mathfrak{p}]$ as above.
- The norm is multiplicative: $N(\mathfrak{A}\,\mathfrak{B}) = N(\mathfrak{A}) \cdot N(\mathfrak{B})$.

From this we see that taking norms in (*) leads to

$$\mathfrak{p}^{[L:K]} = \mathfrak{p}^{e_1 f_1} \dots \mathfrak{p}^{e_s f_s}.$$

Hence the identity similar to the one from theorem 15.7 has form

$$\sum_i e_i f_i = [L : K].$$

Essentially the same formula will appear below in theorem 17.3.

16 Unramified and totally ramified extensions

In this section to simplify things we assume that the fields are complete with respect to a *discrete* valuation. In this case $[L : K] = e_{L/K} \cdot f_{L/K}$.

Definition 16.1. Let L/K be a finite extension of complete fields.

- L/K is **unramified** if $e_{L/K} = 1$, and so $[L : K] = f_{L/K}$.
- L/K is **totally ramified** if $f_{L/K} = 1$, and so $[L : K] = e_{L/K}$.
- L/K is **tamely ramified** if $\operatorname{char} F_K$ does not divide $e_{L/K}$. Otherwise we say that L/K is **wild**.

Proposition 16.2. *Assume F_L/F_K is a separable extension. Given L/K as above, there exists an intermediate field $K \subset L_0 \subset L$ such that L_0/K is unramified and L/L_0 is totally ramified. (This L_0 is actually unique.)*

Proof. Since F_L/F_K is separable, we have $F_L = F_K(\overline{\theta})$ for some $\overline{\theta} \in F_L$. Let $\overline{p}(T) \in F_K[T]$ be the minimal (monic) polynomial of $\overline{\theta}$ over F_K. Let $p(T) \in O_K[T]$ be a monic lifting of $\overline{p}$. The degree of p is $f_{L/K}$, and it is irreducible over K.

Let $\theta_0 \in O_L$ be a lifting of $\overline{\theta} \in F_L$. We have $p(\theta_0) \equiv 0 \pmod{I_L}$ and $p'(\theta_0) \not\equiv 0 \pmod{I_L}$ (because $\overline{p}$ is separable, $\overline{p}'(\theta) \neq 0$). Now apply the Hensel's lemma that says that there exists $\theta \in O_L$ such that $p(\theta) = 0$ and $\theta \equiv \overline{\theta} \pmod{I_L}$.

Take $L_0 := K(\theta)$. We have $F_{L_0} = F_L$ and so $f_{L_0/K} = f_{L/K}$. As for the ramification index, $[L_0 : K] = \deg p = f_{L/K}$, so $e_{L_0/K} = 1$.

$f_{L/L_0} = 1$, so L/L_0 is totally ramified. ∎

Using the Hensel's lemma in the same way as above, we get the following characterization of unramified extensions, assuming F_K is a perfect field.

Theorem 16.3. *Let K be a complete local field. Assume its residue field F_K is perfect. There is 1-1 correspondence between finite extensions F_L/F_K and finite unramified extensions L/K.*

$$\begin{array}{ccc} O_K & \hookrightarrow & O_L \\ \downarrow & & \downarrow \\ F_K & \hookrightarrow & F_L \end{array}$$

Proof. Assume we have an unramified extension L/K. Then we have $F_L := O_L/(\pi_K)$ and $F_K := O_K/(\pi_K)$ and an extension F_L/F_K.

In the other direction, assume we have an extension F_L/F_K. Since F_K is perfect by the assumption, $F_L = F_K(\overline{\theta})$ for some $\overline{\theta} \in F_L$. Let $\overline{p}(X) \in F_K[X]$ be the minimal polynomial of $\overline{\theta}$. Consider a lift $p(X) \in O_K[X]$. It must be irreducible since $\overline{p}$ is irreducible. By Hensel's lemma, there exist a *unique* $\theta \in O_L$ such that $p(\theta) = 0$ and $\theta \equiv \overline{\theta} \pmod{\pi_K}$. Now take $L := K(\theta)$. We have $[L:K] = \deg p = \deg \overline{p} = [F_L : F_K]$, so L/K is unramified. ■

Example 16.4. The field of p-adic numbers $\mathbb{Q}_p$ has $\mathbb{F}_p$ as its residue field. By the theorem above, unramified extensions of $\mathbb{Q}_p$ correspond to finite extensions of $\mathbb{F}_p$. But the latter field has exactly one extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ for each degree n, thus there is a *unique* unramified extension $L_n/\mathbb{Q}_p$ of any given degree n.

It is $L_n = \mathbb{Q}_p(\zeta_{p^n-1})$, obtained by adjoining (p^n-1)-roots of unity. It is a cyclic Galois extension and its Galois group $\mathrm{Gal}(L_n/\mathbb{Q}_p)$ is generated by the Frobenius automorphism ϕ_n which induces the usual Frobenius on $\mathbb{F}_{p^n}/\mathbb{F}_p$:

$$\phi_n(x) \equiv x^{p^n} \pmod{p} \quad \text{for all } x \in O_{L_n}.$$

▲

Example 16.5. Let F be a perfect field. Unramified extensions of $F((T))$ are isomorphic to $\widetilde{F}((T))$ where $\widetilde{F}$ is an extension of F. ▲

Theorem 16.6. *Let L/K be a totally ramified extension of a discrete complete local field. Then $e = e_{L/K} = [L:K]$, and there exists an* ***Eisenstein polynomial***

$$p(T) = T^e + a_{e-1}T^{e-1} + \cdots + a_1 T + a_0, \quad \text{where } v_{\pi_K}(a_0) = 1,\ v_{\pi_K}(a_i) \geq 1 \text{ for } i = 1, \ldots, e-1,$$

such that L is generated by a root of $p(T)$.

Proof. We have $L = K(\pi_L)$. Let $\widetilde{L}$ be a finite Galois extension of K containing L. Let $\pi_L^{(1)}, \ldots, \pi_L^{(e)} \in \widetilde{L}$ be the conjugates of π_L over K.

Claim. *If $\alpha, \beta \in \overline{K}$ are conjugate over K, then $|\alpha| = |\beta|$.*

Indeed, let $\widetilde{L}$ be a finite Galois extension of K containing α and β. Then there exists an automorphism

$$\begin{aligned} \sigma \colon \widetilde{L} &\to \widetilde{L}, \\ \alpha &\mapsto \beta, \end{aligned}$$

fixing K (that is, $\sigma|_K = id$). Since $|\cdot|$ extends uniquely to $\widetilde{L}$, this σ must preserve the absolute value.

So $|\pi_L^{(i)}| = |\pi_L|$. Take $p(T)$ to be the minimal monic polynomial of π_L/K. We have $a_0 = \pm\pi_L^{(1)} \cdots \pi_L^{(e)}$, so $|a_0| = |\pi_L|^e = |\pi_K|$. Similarly the other a_i's are symmetric functions of $\pi_L^{(1)}, \ldots, \pi_L^{(e)}$:

$$\begin{aligned}
a_0 &= (-1)^e \pi_L^{(1)} \pi_L^{(2)} \cdots \pi_L^{(e)}, \\
a_1 &= (-1)^{e-1} (\pi_L^{(1)} \pi_L^{(2)} \cdots \pi_L^{(e-1)} + \pi_L^{(1)} \pi_L^{(2)} \cdots \pi_L^{(e-2)} \pi_L^{(e)} + \ldots + \pi_L^{(2)} \pi_L^{(3)} \cdots \pi_L^{(e)}), \\
&\vdots \\
a_{e-3} &= -(\pi_L^{(1)} \pi_L^{(2)} \pi_L^{(3)} + \pi_L^{(1)} \pi_L^{(2)} \pi_L^{(4)} + \cdots + \pi_L^{(e-2)} \pi_L^{(e-1)} \pi_L^{(e)}), \\
a_{e-2} &= \pi_L^{(1)} \pi_L^{(2)} + \pi_L^{(1)} \pi_L^{(3)} + \cdots + \pi_L^{(1)} \pi_L^{(e)} + \pi_L^{(2)} \pi_L^{(3)} + \cdots + \alpha_{e-1}\, \alpha_e, \\
a_{e-1} &= -(\pi_L^{(1)} + \pi_L^{(2)} + \cdots + \pi_L^{(e)}).
\end{aligned}$$

We have indeed $v_{\pi_K}(a_0) = 1$ and $v_{\pi_K}(a_i) \geq 1$ for $i = 1, \ldots, e-1$. ■

Remark 16.7. Actually, an extension L/K of discrete complete local fields is totally ramified *if and only if* $L = K(\theta)$ with θ being a root of an Eisenstein polynomial.

Proposition 16.8. *Let L/K be a totally ramified tame extension of a discrete complete local field. Then there exists a primitive element π_K of K such that $\pi_L^e = \pi_K$ where $e = e_{L/K} = [L:K]$. (That is, $\pi_L^e = \pi_K$ for these elements, not only $(\pi_L)^e = (\pi_K)$ for the ideals.)*

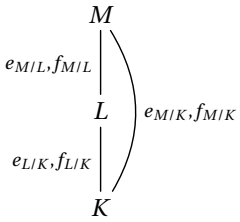
Proof. For π_K and π_L we have $\pi_L^e = \pi_K \eta$ for some $\eta \in O_L^\times$. Since the extension is totally ramified, $F_L = F_K$. So there exists $\theta \in O_K^\times$ such that $\eta \equiv \theta \pmod{\pi_L}$. Replacing π_K with $\pi_K\theta$ and η with $\eta\theta^{-1}$, we may assume $\eta \equiv 1 \pmod{\pi_L}$.

Claim. *If $\operatorname{char} F_L \nmid m$, then every $\alpha \in O_L$ satisfying $\alpha \equiv 1 \pmod{I_L}$ is an m-th power.*

(Indeed, we can apply Hensel to the polynomial $f(X) = X^m - \alpha$ and $\alpha_0 = 1$; by the assumption $f'(\alpha_0) = m \not\equiv 0 \pmod{I_m}$.)

The claim can be applied since L/K is tame. So η is an e-th root, $\eta = \epsilon^e$ for some $\epsilon \in O_L^\times$. Replacing π_L with $\pi_L\epsilon^{-1}$, we obtain $\pi_L^e = \pi_K$. ∎

Lemma 16.9. *Assume we have finite extensions of complete local fields $K \subset L \subset M$.*



Then

$$f_{M/K} = f_{L/K} \cdot f_{M/L},$$
$$e_{M/K} = e_{L/K} \cdot e_{M/L}.$$

In particular, M/K is unramified (totally ramified) iff both M/L and L/K are unramified (totally ramified).

Proof. By definition $e_{L/K} := [\Gamma_L : \Gamma_K]$. We have a chain of subgroups $\Gamma_K \le \Gamma_L \le \Gamma_M$, and

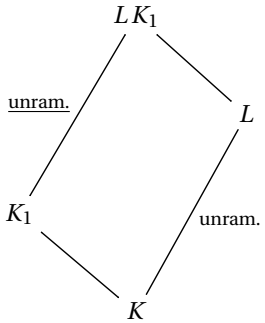
$$[\Gamma_M : \Gamma_K] = [\Gamma_M : \Gamma_L] \cdot [\Gamma_L : \Gamma_K].$$

Now $f_{L/K} := [F_L : F_K]$. We have field extensions $F_K \subset F_L \subset F_M$, and

$$[F_M : F_K] = [F_M : F_L] \cdot [F_L : F_K].$$

∎

Lemma 16.10. *Let L/K be an unramified extension and let K_1/K be a finite extension. Assume F_L/F_K is separable. Then the compositum LK_1/K_1 is unramified.*



Proof. Since F_L/F_K is a finite separable extension, we have $F_L = F_K(\overline{\theta})$ for some $\overline{\theta} \in F_L$. Consider its lifting $\theta \in O_L$ and its minimal polynomial $p(X) \in O_K[X]$. Reduce this polynomial modulo π_K: consider $\overline{p}(X) := p(X) \bmod \pi_K \in F_K[X]$. Now we have, under our assumption that $[L:K] = [F_L : F_K]$,

$$[F_L : F_K] \le \deg \overline{p} = \deg p = [K(\theta) : K] \le [L : K] = [F_L : F_K].$$

Hence $L = K(\theta)$ and $\overline{p}(X)$ is the minimal polynomial of $\overline{\theta}$ over F_K. Thus $LK_1 = K_1(\theta)$.

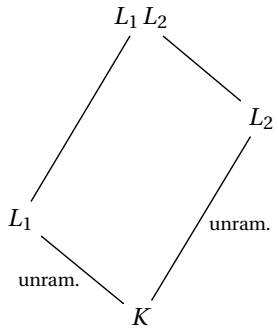
Let $q(x) \in O_{K_1}[X]$ be the minimal polynomial of θ over K_1 and let $\overline{q}(X) := q(X) \pmod{\pi}_K \in F_{K_1}[X]$. This reduced modulo π_K polynomial $\overline{q}(X)$ is separable as a factor of $\overline{p}(X)$, and so it is irreducible over F_{K_1}, because otherwise $q(X)$ would be reducible by Hensel's lemma. Now

$$[F_{LK_1} : F_{K_1}] \le [LK_1 : K_1] = \deg q = \deg \overline{q} = [F_{K_1}(\overline{\theta}) : K_1] = [F_{LK_1} : F_{K_1}].$$

So $[LK_1 : K_1] = [F_{LK_1} : F_{K_1}]$. ■

From these lemmas we have the following:

Proposition 16.11. *Let L_1/K and L_2/K be two unramified extensions. Then their compositum L_1L_2 is unramified as well.*



Proof. Indeed, the extension L_1L_2/L_1 is unramified as well by lemma 16.10, and so L_1L_2/K is unramified by lemma 16.9. ■

So there exists a unique **maximal unramified extension** K^{unr} of a field, given by the compositum of all finite unramified subextensions of K^{alg}/K.

Similarly, if L/K is a finite extension, then, taking the compositum of all its unramified subextensions, we obtain the maximal unramified subextension L_0/K.

Example 16.12. Let $K = F((T))$ where F is a perfect field. Then the maximal unramified extension K^{unr} is smaller than $F^{\mathrm{alg}}((T))$: it is given by series whose coefficients lie in a finite extension of F:

$$K^{\mathrm{unr}} = \{x(T) = \sum_{n\ge 0} a_n T^n \in F^{\mathrm{alg}}((T)) \mid [F(a_0, a_1, \ldots) : F] < \infty\}.$$

This is not a complete field: it is easy to give a Cauchy sequence $(x_n(T))$ not converging to an element of K^{unr}; e.g. one can take

$$x_n(T) := \sum_{0\le k\le n} \sqrt{k}\, T^k.$$

If we consider the completion of K^{unr}, then we obtain $F^{\mathrm{alg}}((T))$. ▲

Example 16.13. The maximal unramified extension of $\mathbb{Q}_p$ is obtained by adjoining all roots of unity ζ_n of order n prime to p (see example 16.4 above; note that $(p,n) = 1$ implies $p^{\phi(n)} - 1 \equiv 0 \pmod{n}$). ▲

17 Absolute values on incomplete fields

We have mentioned before (p. 40) that for an extension of complete fields L/K an absolute value on K uniquely extends to L. Now we drop the assumption that K is complete. Suppose it is a field with an absolute value $|\cdot|_v$ and L/K is a finite extension. How $|\cdot|_v$ extends to L?

For an absolute value $|\cdot|_v$ let K_v be the completion of K with respect to $|\cdot|_v$ and let $\overline{K_v}$ be an algebraic closure of this completion. Now $|\cdot|_v$ extends uniquely on K_v, and then on $\overline{K_v}$. Denote $|\cdot|_{\overline{v}}$ the corresponding absolute value on $\overline{K_v}$ (but be careful: $\overline{K_v}$ is *not* complete with respect to $|\cdot|_{\overline{v}}$).

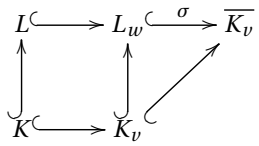
Now for a finite extension L/K we can choose an embedding $\sigma\colon L \to \overline{K_v}$ and using this define an absolute value on L:

$$|x|_w := |\sigma(x)|_{\overline{v}}.$$

One can consider the completion L_w of L with respect to w. There is a (continuous) embedding $\sigma\colon L_w \to \overline{K_v}$ induced by σ:

$$L_w \hookrightarrow \overline{K_v},$$
$$\varprojlim x_n \text{ w.r.t. } |\cdot|_w \mapsto \varprojlim \sigma(x_n) \text{ w.r.t. } |\cdot|_{\overline{v}}.$$

Extending an absolute value $|\cdot|_v$ to L corresponds to choosing an embedding $L \hookrightarrow \overline{K_v}$ because of the following commutative diagram:



For $x \in L_w$ one must have $|x|_w = |\sigma(x)|_{\overline{v}}$.

Example 17.1. The main example is given by the absolute values on number fields.

Let $K = \mathbb{Q}$ and let $L = \mathbb{Q}(\alpha)$ where α is a root of polynomial $T^2 - 2$. Consider the usual archimedian absolute value $|\cdot|_\infty$ on $\mathbb{Q}$. It extends uniquely to $\mathbb{C}$. There are two embeddings of L in $\mathbb{C}$, given by two roots of $T^2 - 2$:

$$\sigma_{1,2}\colon L \to \mathbb{C},$$
$$\sigma_1\colon \alpha \mapsto +\sqrt{2},$$
$$\sigma_2\colon \alpha \mapsto -\sqrt{2}.$$

And this gives rise to two distinct absolute values

$$|x|_{w_1} := |\sigma_1(x)|_\infty, \quad |x|_{w_2} := |\sigma_2(x)|_\infty.$$

They indeed differ: for the element $x = 1 + \alpha$ one has $|x|_{w_1} = 1 + \sqrt{2}$ and $|x|_{w_2} = \sqrt{2} - 1$.

Now let α be a root of $T^2 + 1$. Then the embeddings are

$$\sigma_{1,2}\colon \alpha \mapsto \pm i.$$

But σ_1 and σ_2 give rise to the same absolute value, because they are conjugate by the action of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$! ▲

Now let L/K be a field extension of degree $n = [L : K]$. Then there are n distinct embeddings

$$\sigma_i\colon L \hookrightarrow \overline{K_v},$$

leaving K fixed.

Each σ_i gives rise to an extension of $|\cdot|_v$ to L, and every extension of an absolute value is obtained this way. So we see that there are *at most n* extensions of an absolute value on K. However, the last example shows that distinct embeddings $L \hookrightarrow \overline{K_v}$ can give rise to the same absolute value.

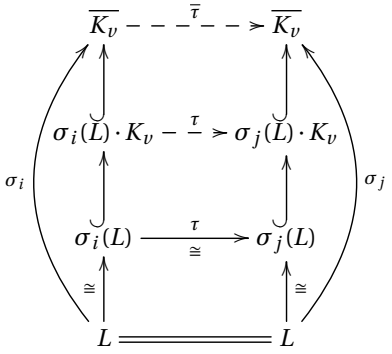
Theorem 17.2. *Let $\sigma_1, \dots, \sigma_n$ be embeddings $L \hookrightarrow \overline{K_v}$ fixing K. Consider the following equivalence relation: $\sigma_i \sim \sigma_j$ if there is $\tau \in \mathrm{Gal}(\overline{K_v}/K_v)$ such that $\sigma_j = \tau \circ \sigma_i$.*

$$L \xhookrightarrow{\sigma_i} \overline{K_v} \xrightarrow{\tau} \overline{K_v}, \qquad L \xhookrightarrow{\sigma_j} \overline{K_v}$$

There is one-to-one correspondence between extensions of $|\cdot|_v$ to L and equivalence classes of embeddings $\sigma_i \colon L \hookrightarrow \overline{K_v}$.

Proof. It is clear that equivalent embeddings give rise to the same absolute values. Indeed, $|\sigma(x)|_{\overline{v}} = |\tau\sigma(x)|_{\overline{v}}$ since conjugate elements have the same absolute value.

Now consider two embeddings $\sigma_i, \sigma_j \colon L \to \overline{K_v}$ such that $|\sigma_i(\cdot)|_{\overline{v}} = |\sigma_j(\cdot)|_{\overline{v}}$. We want to show that σ_i and σ_j are conjugate. Consider the isomorphism $\tau \colon \sigma_i(L) \to \sigma_j(L)$ given by $\tau := \sigma_j \circ \sigma_i^{-1}$. We extend this to an isomorphism $\tau \colon \sigma_i(L) \cdot K_v \to \sigma_j(L) \cdot K_v$, and then to $\overline{\tau} \colon \overline{K_v} \to \overline{K_v}$ leaving K_v fixed.



$\sigma_i(L)$ is dense in $\sigma_i(L) \cdot K_v$, so every element $x \in \sigma_i(L) \cdot K_v$ can be written as a limit

$$x = \varprojlim_{n \to \infty} \sigma_i(x_n)$$

for some sequence (x_n) which belongs to a finite subextension of L. Now since $|\sigma_i(\cdot)|_{\overline{v}} = |\sigma_j(\cdot)|_{\overline{v}}$, the sequence

$$\varprojlim_{n \to \infty} \sigma_j(x_n) = \varprojlim_{n \to \infty} \tau(\sigma_i(x_n))$$

converges to some element $\tau(x)$ in $\sigma_j(L) \cdot K_v$. This correspondence gives a well-defined isomorphism

$$\begin{aligned} \tau \colon \sigma_i(L) \cdot K_v &\to \sigma_j(L) \cdot K_v, \\ x &\mapsto \tau(x) \end{aligned}$$

(we check that it does not depend on the choice of the sequence (x_n)), which leaves K_v fixed. This extends to an automorphism $\overline{\tau} \in \mathrm{Gal}(\overline{K_v}/K_v)$, and $\sigma_j = \overline{\tau} \circ \sigma_i$. ∎

Let L/K be a separable extension, so $L = K(\alpha)$. Let $f(T)$ be the minimal polynomial of α, having roots $\alpha_1, \dots, \alpha_n$ in $\overline{K_v}$. Then there are n embeddings

$$\begin{aligned}\sigma_i \colon L &\to \overline{K_v},\\ \alpha &\mapsto \alpha_i.\end{aligned}$$

Now pairwise nonequivalent embeddings correspond to roots α_i that are pairwise nonconjugate over K_v. This means that over K_v the minimal polynomial factors into irreducible polynomials

$$f(T) = f_1(T)\cdots f_s(T),$$

where α_i is a root of f_i. So picking roots of $f_1(T),\dots,f_s(T)$, we obtain different extensions of the absolute value $|\cdot|_{w_1},\dots,|\cdot|_{w_s}$. One has $\deg f_i = [K_v(\alpha_i) : K_v]$.

Theorem 17.3. *Let L/K be a finite separable extension and let $|\cdot|_v$ be an absolute value on K. Let $|\cdot|_{w_1},\dots,|\cdot|_{w_s}$ be extensions of $|\cdot|_v$ to L. Then*

$$\sum_{1\le i\le s} [K_v(\alpha_i) : K_v] = [L : K].$$

Indeed,

$$\sum_{1\le i\le s} [K_v(\alpha_i) : K_v] = \sum_{1\le i\le s} \deg f_i = \deg f.$$

So *the sum of local degrees equals the global degree.* This is a principle occurring in many areas of mathematics! See the remark on p. 43 for an example in the number field case.

Part III
Skolem–Mahler–Lech theorem

In § 19 we are going to see another interesting theorem which is proved using p-adic numbers. We will need to work with expressions like "λ^n", but in the p-adic setting, where both λ and n are p-adic numbers. To make sense of this, we can introduce exponential and logarithm and put "λ^n" $= \exp(n \log \lambda)$. As usual (for $p = \infty$) these can be defined using the well-known power series, but we need some work to establish convergency and basic properties.

18 Nonarchimedian logarithm and exponential

Now let K be a complete nonarchimedian local field of characteristic 0 (we will manipulate with power series having n or $n!$ in denominator, so this restriction is vital). Let F_K be its residue field, having characteristic $\operatorname{char} F_K = p > 0$.

We have the minimal subfield $\mathbb{Q} \subset K$, and since K is complete with $\operatorname{char} F_K = p$, the absolute value on K restricted to $\mathbb{Q}$ is p-adic, thus K contains $\mathbb{Q}_p$. We normalize the absolute value to coincide with the standard p-adic absolute value on $\mathbb{Q}_p$, i.e. $|p|_v = |p|_p = \frac{1}{p}$.

In the subsequent proofs we will need an upper bound on the p-adic valuation $\nu_p(n!)$ of a factorial. First, it is easy to see that

$$\nu_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots \tag{*}$$

This is better to demonstrate by a concrete example. Suppose we want to compute $\nu_2(10!)$. Then we should count all even numbers $2,4,6,8,10$, two numbers $4,8$ divisible by 2^2, and number 8 divisible by 2^3, so totally $\nu_2(10!) = 5+2+1 = 8$.

Example 18.1. Let us calculate how many zeros there are at the end of the decimal expansion of 100!, which is a huge number.

$$\nu_5(100!) = \underbrace{\left\lfloor \frac{100}{5} \right\rfloor}_{20} + \underbrace{\left\lfloor \frac{100}{5^2} \right\rfloor}_{4} = 24.$$

$$\nu_2(100!) = \underbrace{\left\lfloor \frac{100}{2} \right\rfloor}_{50} + \underbrace{\left\lfloor \frac{100}{2^2} \right\rfloor}_{25} + \underbrace{\left\lfloor \frac{100}{2^3} \right\rfloor}_{12} + \underbrace{\left\lfloor \frac{100}{2^4} \right\rfloor}_{6} + \underbrace{\left\lfloor \frac{100}{2^5} \right\rfloor}_{3} + \underbrace{\left\lfloor \frac{100}{2^6} \right\rfloor}_{1} = 97.$$

So we conclude that there are $\min\{\nu_5(100!), \nu_2(100!)\} = 24$ zeros at the end. ▲

The sum (*) appears to be infinite, but of course it ends with zero terms, since we take $\lfloor \cdot \rfloor$. Looking at the corresponding infinite sum, we obtain a strict upper bound

$$\nu_p(n!) < n\left(\frac{1}{p} + \frac{1}{p^2} + \cdots\right) = \frac{n}{p-1}.$$

The same inequality for absolute values looks like

$$|n!|_p > \rho_p^n, \quad \text{where } \rho_p = p^{-\frac{1}{p-1}}.$$

We will need a similar bound (with non-strict inequality):

Lemma 18.2.

$$\nu_p(n!) \le \frac{n-1}{p-1}.$$

That is, $|n!|_p \ge \rho_p^{n-1}$.

Proof. For $n = 2$ we obviously have $v_2(2!) = 1$ and $v_p(2!) = 0$ for $p > 2$, so the lemma holds.
If $p \nmid n$, then $v_p(n) = 0$ and by induction $v_p(n!) = v_p((n-1)!) \le \frac{n-1}{p-1}$.

If $p \mid n$ but $p^2 \nmid n$, then $v_p(n) = 1$. Observe that

$$n! = (n-p)! \cdot \underbrace{(n-p+1)\cdots(n-1)}_{\text{not divisible by } p} \cdot n,$$

so we get (using $v_p((n-p)!) < \frac{n-p}{p-1}$)

$$v_p(n!) = v_p((n-p)!) + 1 \le \frac{n-p}{p-1} + 1 = \frac{n-1}{p-1}.$$

If $v_p(n) = 2$, then

$$n! = (n-p^2)! \cdot \underbrace{(n-p^2+1)\cdots(n-1)\cdot n}.$$

The multipliers $(n-p^2+1)$, $(n-p^2+2)$, …, $n-1$, n in the "tail" modulo p^2 give $1, 2, \ldots, p^2-1, 0$. One has

$$v_p(n!) = v_p((n-p^2)!) + (p-1) + 2 \le \frac{n-p^2}{p-1} + p + 1 = \frac{n-1}{p-1}.$$

. . . . .

Along the same lines, for $v_p(n) = k$ one gets

$$v_p(n!) = v_p((n-p^k)!) + p^{k-1} + p^{k-2} + \cdots + p + 1 \le \frac{n-p^k}{p-1} + \frac{p^k-1}{p-1} = \frac{n-1}{p-1}.$$

■

Remark 18.3. One can also show the following: if n has p-adic expansion $a_0 + a_1\, p + a_2\, p^2 + \cdots + a_k\, p^k$, then

$$v_p(n!) = \frac{n - (a_0 + \cdots + a_k)}{p-1}.$$

Since among $a_0, \ldots, a_k$ at least one is nonzero, this gives the bound that we just proved.

Definition 18.4. The **exponential** of $z \in K$ is given by the power series

$$\exp(z) := \sum_{n \ge 0} \frac{z^n}{n!}.$$

For $|z|_p < \rho_p$ this series converges, since in this case

$$\left|\frac{z^n}{n!}\right| < \left(\frac{|z|}{\rho_p}\right)^n \xrightarrow{n\to\infty} 0.$$

So we consider the exponential on the disk $D(0, \rho_p)$ centered in 0 having radius ρ_p. Observe that $D(0, \rho_p)$ is a group under addition, since $|z_1| < \rho_p$ and $|z_2| < \rho_p$ implies $|z_1 + z_2| < \rho_p$.

The usual properties of exponential hold—because they are proved by formal manipulations with power series. For instance,

$$\exp(z_1) \cdot \exp(z_2) = \exp(z_1 + z_2) \quad \text{for } z_1, z_2 \in D(0, \rho_p).$$

Indeed,

$$\begin{aligned}\exp(z_1)\cdot\exp(z_2) &= \left(\sum_{k\geq 0}\frac{z_1^k}{k!}\right)\cdot\left(\sum_{\ell\geq 0}\frac{z_2^\ell}{\ell!}\right)\\ &= \sum_{n\geq 0}\sum_{k+\ell=n}\frac{n!}{n!}\frac{z_1^k}{k!}\frac{z_2^\ell}{\ell!}\\ &= \sum_{n\geq 0}\frac{1}{n!}\sum_{k\geq 0}\binom{n}{k}z_1^k z_2^{n-k}\\ &= \sum_{n\geq 0}\frac{(z_1+z_2)^n}{n!} = \exp(z_1+z_2).\end{aligned}$$

In particular, $\exp(-z)=\exp(z)^{-1}$, and we have a group homomorphism

$$\exp\colon (D(0,\rho_p),+)\to K^\times.$$

Lemma 18.5. *For $z\in D(0,\rho_p)$ one has $|\exp(z)-1|_p = |z|_p$.*

Proof. Consider

$$\exp(z)-1 = z+\sum_{n\geq 2}\frac{z^n}{n!}. \tag{*}$$

We claim that each sum term has p-adic absolute value less than $|z|_p$. Indeed,

$$\left|\frac{z^n}{n!}\right|_p = |z|_p\cdot\left|\frac{z^{n-1}}{n!}\right|_p \leq |z|_p\cdot\left(\frac{|z|_p}{\rho_p}\right)^{n-1} < |z|_p$$

(where we use the bound $|n!|_p\geq \rho_p^{n-1}$ proved above). Now taking absolute values of the left hand side and the right hand side of (*), we are done. ∎

From this we see that

$$\exp(z)=1 \iff z=0 \quad \text{for } z\in D(0,\rho_p),$$

so the exponential is a monomorphism $(D(0,\rho_p),+)\hookrightarrow K^\times$. Moreover, the inequality

$$|\exp(z)-1|_p = |z|_p < \rho_p$$

means that the image of exponential is in $D(1,\rho_p)$, and the latter is a group under multiplication: if $|z_1-1|_p<\rho_p$ and $|z_2-1|_p<\rho_p$, then $|z_1z_2-1|_p<\rho_p$ and $|z_1^{-1}-1|<\rho_p$.

So we can look at the exponential as a group homomorphism

$$\exp\colon (D(0,\rho_p),+)\to (D(1,\rho_p),\cdot).$$

Our goal is to show that this is actually an isomorphism, that is, to find the inverse to the exponential. But as we know, the inverse is the logarithm!

Definition 18.6. For $z\in K$ the **logarithm** is given by the power series

$$\log(z) := \sum_{n\geq 1}(-1)^{n-1}\frac{(z-1)^n}{n}.$$

This series converges for $|z-1|_p<1$. To see this, recall some analysis.

Proposition 18.7. *For a p-adic power series $\sum_{n\geq 0}\alpha_n z^n$ the **radius of convergence** is given by*

$$r := \frac{1}{\limsup |\alpha_n|_p^{1/n}}.$$

1. *The series converges if $|z|_p < r$.*
2. *The series diverges if $|z|_p > r$.*
3. *If the series converges (diverges) for some z_0 with $|z_0|_p = r$, then it converges (diverges) for all z with $|z|_p = r$.*

Proof. This is because one has

$$|\alpha_n z^n|_p = |\alpha_n|_p \cdot |z|_p^n \geq \left(\frac{|z|_p}{r}\right)^n.$$

■

Example 18.8. Let's compute the radius of convergence for the power series

$$\exp(z) := \sum_{n\geq 0} \frac{z^n}{n!}, \quad \log(z+1) := \sum_{n\geq 1} (-1)^{n-1}\frac{z^n}{n}.$$

For the exponential we get

$$\limsup \left|\frac{1}{n!}\right|_p^{1/n} = \limsup \left(p^{\frac{n-s(n)}{p-1}}\right)^{1/n},$$

where $s(n)$ is the sum of p-adic digits of n (remark 18.3 above), so

$$\limsup \left|\frac{1}{n!}\right|_p^{1/n} = \limsup p^{\frac{1-s(n)/n}{p-1}} = p^{\frac{1}{p-1}},$$

and the radius of convergence for the exponential is $p^{-\frac{1}{p-1}} =: \rho_p$.

For the logarithm

$$\limsup \left|\frac{1}{n}\right|_p^{1/n} = \limsup p^{\nu_p(n)/n} = 1,$$

so the radius of convergence is 1. ▲

Our p-adic logarithm has the expected properties, e.g.

$$\log(z_1 z_2) = \log(z_1) + \log(z_2).$$

The series converges on $D(1,1)$; however, defined on this domain, the logarithm has a nontrivial kernel.

Example 18.9. Let $p = 2$. Then $-1 \in D(1,1)$ since $|-1-1|_p = \frac{1}{2}$. Now

$$\log(-1) + \log(-1) = \log((-1)\cdot(-1)) = \log 1 = 0,$$

thus $\log(-1) = 0$. Similarly, if $\zeta_p \in \overline{\mathbb{Q}_p}$ is a p-th root of unity, then $\log\zeta_p = 0$. ▲

To fix the issue, we look at the logarithm on the disk $D(1,\rho_p)$.

Proposition 18.10. *If $|z-1|_p < \rho_p$, then $|\log z|_p = |z-1|_p$. In particular, $\log z = 0$ iff $z = 1$ on $D(1,\rho_p)$.*

(Actually, $|\zeta_p - 1|_p = \rho_p$, so the proposition cannot be improved.)

Lemma 18.11. *If $0 < |z|_p < \rho_p$, then $\left|\frac{z^n}{n}\right|_p < |z|_p$ for $n \geq 2$.*

This lemma implies immediately the proposition, because one can take absolute values of the equation

$$\log z = (z-1) + \sum_{n\geq 2} (-1)^{n-1} \frac{(z-1)^n}{n}.$$

Proof of the lemma. Assume $1 < n < p$. Then $|n|_p = 1$ and

$$\left|\frac{z^n}{n}\right|_p = |z|_p^n < |z|_p.$$

Now assume $n \geq p$. Then

$$n^{\frac{1}{n-1}} \leq p^{\frac{1}{p-1}}.$$

Next (using $|n|_p \geq n^{-1}$)

$$\left|\frac{z^n}{n}\right|_p = |z|_p \cdot \left|\frac{z^{n-1}}{n}\right|_p \leq |z|_p \cdot n \cdot |z|_p^{n-1} < |z|_p \left(n^{\frac{1}{n-1}}\,\rho_p\right)^{n-1} = |z|_p \left(\frac{n^{\frac{1}{n-1}}}{p^{\frac{1}{p-1}}}\right)^{n-1} \leq |z|_p.$$

■

Further, by manipulations with power series we can check that

$$\begin{aligned} \log\exp z &= z, \quad \text{for } |z|_p < \rho_p, \\ \exp\log z &= z, \quad \text{for } |z-1|_p < \rho_p. \end{aligned}$$

Thus we finally obtained a group isomorphism

$$D(0,\rho_p) \underset{\log}{\overset{\exp}{\rightleftarrows}} D(1,\rho_p)$$

If $\operatorname{char} F_K = 0$, then one can define $\exp(z)$ for $|z| < 1$ and $\log(z)$ for $|z-1| < 1$, giving an isomorphism $D(0,1) \cong D(1,1)$.

19 Skolem–Mahler–Lech theorem

We are going to discuss certain properties of the so-called "linear recurrences".

Definition 19.1. A sequence of complex numbers $(u_n)_{n\in\mathbb{Z}}$, $u_n \in \mathbb{C}$ is called a **linear recurrence** of order m if there exist numbers $\alpha_0, \ldots, \alpha_m \in \mathbb{C}$, where $\alpha_0, \alpha_m \neq 0$, such that for all $n \in \mathbb{Z}$

$$\alpha_0 u_n + \alpha_1 u_{n+1} + \cdots + \alpha_m u_{n+m} = 0.$$

Example 19.2. Probably the most famous example are the **Fibonacci numbers**. They are defined by a linear relation $u_n + u_{n+1} - u_{n+2} = 0$ and we set $u_0 := 0$, $u_1 := 1$.

$\cdots$	u_{-5}	u_{-4}	u_{-3}	u_{-2}	u_{-1}	u_0	u_1	u_2	u_3	u_4	u_5	$\cdots$
$\cdots$	5	-3	2	-1	1	0	1	1	2	3	5	$\cdots$

▲

For a linear recurrence (u_n) we are interested in the set $\{n \in \mathbb{Z} \mid u_n = 0\}$. We will say that it is the **solution** of the equation $u_n = 0$ (with respect to n). In the case of Fibonacci numbers, this is just $\{0\}$. But of course this can be an infinite set as well.

Example 19.3. A linear recurrence given by $u_{n+2} - u_n = 0$ and $u_0 := 0$, $u_1 := 1$ is the sequence

$$u_n = \begin{cases} 0, & n \text{ even}, \\ 1, & n \text{ odd}. \end{cases}$$

In this case the solution is $2\mathbb{Z}$. Similarly, for any $N = 1, 2, 3, \ldots$ and $a \in \mathbb{Z}$, the set $a + N\mathbb{Z}$ can occur as a solution. ▲

If (u_n) and (v_n) are linear recurrences, then $(u_n v_n)$ and $(u_n + v_n)$ are linear recurrences as well. If A is the solution of (u_n) and B is the solution of (v_n), then $A \cup B$ is the solution of $(u_n v_n)$.

Remark 19.4. The following are equivalent:

(1) (u_n) is a linear recurrence, i.e. it is given by relations $\alpha_0 u_n + \alpha_1 u_{n+1} + \cdots + \alpha_m u_{n+m} = 0$.

(2) $u_n = \sum_{1 \le i \le s} p_i(n) \lambda_i^n$ for some numbers $\lambda_i \in \mathbb{C}$ and polynomials $p_i \in \mathbb{C}[X]$.

(3) The generating function $\sum_{n \ge 0} u_n X^n$ is rational, i.e. equal to $\frac{p(X)}{q(X)}$ for some $p, q \in \mathbb{C}[X]$.

In particular, the implication (1) ⇒ (2) will be seen below. From (2) it is clear why for linear recurrences (u_n) and (v_n) the product $(u_n v_n)$ is again a linear recurrence. Observe that for (3) this gives an interesting property: if $\sum_{n \ge 0} u_n X^n$ and $\sum_{n \ge 0} v_n X^n$ are rational generating functions, then their "Hadamard product" $\sum_{n \ge 0} u_n v_n X^n$ is rational as well.

From the example above we see that a linear recurrence can give a solution which is a finite union of "residue classes" $a + N\mathbb{Z}$. Also some finite set trivially can be a solution. Is it possible to have something more sophisticated? For instance, can there be a linear recurrence having as its solution the squares $1, 4, 9, 16, 25, \ldots$, or the primes $2, 3, 5, 7, 11, \ldots$? The answer is *no*.

Theorem 19.5 (Skolem–Mahler–Lech)**.** *Let (u_n) be a linear recurrence. Then there exists $N \in \mathbb{Z}_{\ge 1}$ and $S \subseteq \{0, 1, \ldots, N-1\}$ (possibly $S = \emptyset$) and a finite set $T \subset \mathbb{Z}$ such that*

$$u_n = 0 \iff n \in T \cup (S + N\mathbb{Z}).$$

The theorem is named after a Norwegian mathematician Thoralf Skolem (who gave a proof for linear recurrences over $\mathbb{Q}$; 1933), a German mathematician Kurt Mahler (who gave a proof for $\overline{\mathbb{Q}}$; 1935), and a Swedish mathematician Christer Lech (who gave a proof for any field of characteristic 0). For historical matters see *Christer Lech, A note on recurring series, Arkiv för Matematik 2 (1953), issue 5, 417–421*, http://dx.doi.org/10.1007/BF02590997

We are going to see a very interesting proof which uses p-adic analysis. We start with some general facts about linear recurrences.

Example 19.6. Recall that for the Fibonacci sequence we have the formulas giving the n-th term explicitly:

$$u_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}, \quad \alpha := \frac{1 + \sqrt{5}}{2}, \ \beta := \frac{1 - \sqrt{5}}{2}.$$

▲

We can write down such a formula for any linear recurrence.

Fix $\alpha_0, \ldots, \alpha_m \in \mathbb{C}$ and let

$$U := \{(u_n)_{n \in \mathbb{Z}} \mid \alpha_0 u_n + \cdots + \alpha_m u_{n+m} = 0\}.$$

This is a $\mathbb{C}$-vector space of dimension m, since each sequence is completely determined by $u_0, \ldots, u_{m-1}$. We are interested in a nice basis for U.

Consider the polynomial $\chi(T) = \alpha_m T^m + \cdots + \alpha_1 T + \alpha_0$. If λ is a root of $\chi(T)$, then $(\lambda^n)_{n \in \mathbb{Z}} \in U$, because

$$\alpha_m \lambda^{n+m} + \alpha_{m-1} \lambda^{n+m-1} + \cdots + \alpha_0 = \lambda^n \chi(\lambda) = 0.$$

If $\chi(T)$ has m *distinct* roots $\lambda_1, \ldots, \lambda_m$, then $\{(\lambda_i^n)\}_{1 \le i \le m}$ forms a basis of U. Assume now that λ is a *multiple* root of $\chi(T)$, i.e. $\chi(\lambda) = \chi'(\lambda) = 0$. Then the polynomial $T^n \chi(T)$ also has λ as a multiple root, so $(T^n \chi(T))'_{T=\lambda} = 0$.

$$\alpha_m (n+m) \lambda^{n+m-1} + \alpha_{m-1} (n+m-1) \lambda^{n+m-2} + \cdots + \alpha_0 n \lambda^{n-1} = 0.$$

So $(n\lambda^{n-1}) \in U$, and also $(n\lambda^n) \in U$. If λ is a root of order ≥ 3, then $(n^2 \lambda^n) \in U$, and so on. If λ is a root of order μ, then $(n^k \lambda^n) \in U$ for $k = 0, 1, \ldots, \mu - 1$. Thus when $\chi(T)$ has roots $\lambda_1, \ldots, \lambda_s$ of order $\mu_1, \ldots, \mu_s$ (with $\mu_1 + \cdots + \mu_s = m$), there is a basis of U given by $(n^k \lambda_i^n)_{0 \le k \le \mu_i - 1}^{1 \le i \le s}$.

Theorem 19.7. *Let (u_n) be a linear recurrence of order m. Then there exist numbers $\lambda_1, \ldots, \lambda_s$ and polynomials $p_1(T), \ldots, p_s(T)$ with $\sum_{1 \le i \le s} (\deg p_i + 1) \le m$ such that*

$$u_n = p_1(n) \lambda_1^n + \cdots + p_s(n) \lambda_s^n.$$

From now on we are going to work with recurrences of this form. So the fact that is equivalent to the Skolem–Mahler–Lech theorem is the following.

Let $p_1(T), \ldots, p_s(T) \in \mathbb{C}[T]$ be some polynomials and let $\lambda_1, \ldots, \lambda_s \in \mathbb{C}^\times$ be pairwise distinct numbers. Then there exists $N \in \mathbb{Z}_{\ge 1}$ and $S \subset \{0, 1, \ldots, N-1\}$ together with a finite set $T \subset \mathbb{Z}$ such that

$$p_1(n) \lambda_1^n + \cdots + p_s(n) \lambda_s^n = 0 \iff n \in T \cup (S + N\mathbb{Z}).$$

We will prove this under an additional assumption that $p_s(T) \in \overline{\mathbb{Q}}[T]$ and $\lambda_1, \ldots, \lambda_s \in \overline{\mathbb{Q}}^\times$. The general case can be reduced to this, but we are not going to discuss the reduction.

Under our assumption, there is some number field K such that $p_i(T) \in K[T]$ and $\lambda_i \in K^\times$. The rough idea of the proof is that one can consider the equation

$$u(n) := p_1(n) \lambda_1^n + \cdots + p_s(n) \lambda_s^n = 0,$$

but treating $u(n)$ as an analytic function on $\mathbb{Z}_p$, not as a function on $\mathbb{Z}$. For this one should make sense of taking exponents "λ_i^n". Of course "$\lambda_i^n = \exp(n \log \lambda_i)$", and we have seen what is the exponential and logarithm in the nonarchimedian setting. However, log is defined only on the disk $D(1, \rho_p)$, and this is a problem one has to fix.

Let us make it precise what an analytic function is.

Definition 19.8. Let K be a complete nonarchimedian field. A function $f \colon D(a, r) \to K$ on some disk of radius r with center in a is called **analytic** if

$$f(z) = \sum_{k \ge 0} \alpha_k (z - a)^k,$$

where the series converges for all $z \in D(a, r)$.

We need the following property of analytic functions:

Proposition 19.9. *Assume that f is not identically zero. Then the set of zeros of f is discrete, in the sense that if $f(z_0) = 0$, then $f(z) \ne 0$ in a punctured neighborhood of z_0.*

Using the compactness of $\mathbb{Z}_p$, we obtain from this the following.

Corollary 19.10. *Let f be an analytic function on $\mathbb{Z}_p$, not identically zero. Then it has at most finitely many zeros.*

Now we go back to the Skolem–Mahler–Lech theorem. We have a function $u(n) := p_1(n) \lambda_1^n + \cdots + p_s(n) \lambda_s^n$ with $\lambda_1, \ldots, \lambda_s \in K^\times$ and $p_1(T), \ldots, p_s(T) \in K[T]$. There exists a nonarchimedian absolute value $|\cdot|_v$ on K such that

$$|\lambda_1|_v = \cdots = |\lambda_s|_v = 1.$$

This v extends the p-adic absolute value on $\mathbb{Q}$. The completion K_v with respect to $|\cdot|_v$ is a finite extension of $\mathbb{Q}_p$. We want $\log \lambda_i$ to be defined, and for this we need $|\lambda_i - 1|_v < \rho_p = p^{-\frac{1}{p-1}}$.

Let $\mathfrak{p}_v$ be the prime ideal of O_{K_v}. Then $|\lambda - 1|_v < \rho_p$ is equivalent to $\lambda \equiv 1 \pmod{\mathfrak{p}_v^m}$ for some $m \in \mathbb{Z}_{\geq 1}$, i.e. to the fact that the image of λ in the finite ring $O_{K_v}/\mathfrak{p}_v^m$ is 1. Since $|\lambda|_v = 1$, we have $\lambda \in O_{K_v}^\times$. By the Fermat's little theorem,

$$\lambda^N \equiv 1 \pmod{\mathfrak{p}_v^m}, \quad \text{where } N = \#(O_{K_v}/\mathfrak{p}_v^m)^\times.$$

So $\lambda_1^N, \ldots, \lambda_s^N$ lie in the disk $D(1, \rho_p)$. For each number $r \in \{0, 1, \ldots, N-1\}$ we can put

$$u_r(z) := \sum_{1 \leq i \leq s} p_i(r + Nz)\, \lambda_i^r \exp(z \log \lambda_i^N).$$

This is well-defined for $z \in \mathbb{Z}_p$. If $n \equiv r \pmod{N}$, then $n = r + Nk$ such that $u(n) = u_r(k)$.

$$\begin{aligned} u_r(k) &= \sum_{1 \leq i \leq s} p_i(r + Nk)\, \lambda_i^r \exp(k \log \lambda_i^N) \\ &= \sum_{1 \leq i \leq s} p_i(n)\, \lambda_i^r \exp(\log \lambda_i^{Nk}) \\ &= \sum_{1 \leq i \leq s} p_i(n)\, \lambda_i^r\, \lambda_i^{Nk} \\ &= \sum_{1 \leq i \leq s} p_i(n)\, \lambda_i^n = u(n). \end{aligned}$$

Now fix r. There are two cases.

1. $u_r(z)$ is identically 0. Then $u(n) = 0$ for $n \equiv r \pmod{N}$. This corresponds to $r \in S$ in the theorem.
2. $u_r(z)$ is not identically 0. Then $u(n) = 0$ for finitely many $n \equiv r \pmod{N}$. This corresponds to the finite set T in the theorem.

So these considerations finish our proof of the Skolem–Mahler–Lech theorem. An interesting feature of it is that we use properties of analytic nonarchimedian functions to conclude that T is some finite set, but we do not construct T explicitly. All the proofs known thus far are not effective in this sense, apart from some particular cases.

Part IV
Sprindžuk's theorem

20 Statement of Sprindžuk's theorem

We are going to discuss a theorem of a Belarusian mathematician V. G. Sprindžuk (1936–1987), which is related to the following classical result.

Theorem 20.1 (Hilbert's irreducibility theorem)**.** *Let $F(X,T) \in \mathbb{Q}[X,T]$ be a polynomial irreducible over $\mathbb{Q}$. Then there exist infinitely many integers $\tau \in \mathbb{Z}$ such that $F(X,\tau) \in \mathbb{Q}[X]$ is irreducible.*

Example 20.2. Consider a polynomial $F(X,T) = X^2 - T$. The polynomial $F(X,\tau)$ is irreducible iff τ is not a square. So the theorem says there are infinitely many nonsquares (which is not surprising). ▲

But in fact, a stronger result holds. Consider the set

$$H_F := \{\tau \in \mathbb{Z} \mid F(X,\tau) \text{ is irreducible}\}.$$

It is not just infinite, but has density 1. That is,

$$\frac{\#(H_F \cap [-x,x])}{2\cdot x} \xrightarrow{x\to\infty} 1;$$

for instance, a big random number is almost never a square. It is harder to show but still true is that $\#(H_F \cap [0,x]) = x + O(x^{1/2})$.

Our ultimate goal is to prove the following fact:

Theorem 20.3 (Sprindžuk's irreducibility theorem)**.** *Let $F(X,T) \in \mathbb{Q}[X,T]$ be a polynomial irreducible over $\mathbb{Q}$. Further assume that*

1. *$F(0,0) = 0$, so that F has no free term.*
2. *$F'_X(0,0) \neq 0$, so that some term is linear in X.*

Then for all but finitely many primes p the polynomial $F(X,p)$ is irreducible over $\mathbb{Q}$.

One can refine the statement above and replace primes p with prime powers p^k, so that $F(X,p^k)$ is irreducible for all but finitely many prime powers p^k. Further, one can show that $F(X,\frac{1}{n})$ is irreducible for all but finitely many $n \in \mathbb{Z}$. We put this together and restate the theorem.

Theorem 20.4 (Sprindžuk's irreducibility theorem II)**.** *Let $F(X,T) \in \mathbb{Q}[X,T]$ be a polynomial irreducible over $\mathbb{Q}$. Assume $F(0,0) = 0$ and $F'_X(0,0) \neq 0$.*

Consider the set

$$\Omega := \{p^k \mid p \text{ is prime}, k = 1,2,3,\ldots\} \cup \{\frac{1}{n} \mid n = 2,3,4,\ldots\}.$$

Then $F(X,\alpha) \in \mathbb{Q}[X]$ is irreducible over $\mathbb{Q}$ for all but finitely many $\alpha \in \Omega$.

Observe that the elements of Ω satisfy the following property: for $\alpha \in \Omega$ one has $|\alpha|_\nu < 1$ exactly for one place $\nu \in M_\mathbb{Q} = \{2,3,5,\ldots,\infty\}$ (possibly the infinite one). Denote

$$S_\alpha := \{\nu \in M_\mathbb{Q} \mid |\alpha|_\nu < 1\}.$$

For $\alpha = p^k$ we have $S_\alpha = \{p\}$, and for $\alpha = \frac{1}{n}$ we have $S_\alpha = \{\infty\}$.

Example 20.5. Consider $\alpha = -\frac{12}{5}$. Then $S_\alpha = \{2,3\}$.
For $\alpha = -\frac{5}{12}$ one has $S_\alpha = \{5,\infty\}$.
For $\alpha = \frac{3}{2}$ one has $S_\alpha = \{3\}$—in particular, we see that $\{\alpha \mid |S_\alpha| = 1\} \supsetneq \Omega$. ▲

A more general result due to Sprindžuk is the following:

Theorem 20.6 (Sprindžuk's decomposition theorem)**.** *Let $F(X,T) \in \mathbb{Q}[X,T]$ be a polynomial irreducible over $\mathbb{Q}$. Assume $F(0,0) = 0$ and $F'_X(0,0) \neq 0$. Let $\epsilon > 0$. For $\alpha \in \mathbb{Z}$ write down the factorization of $F(X,\alpha) \in \mathbb{Q}[X]$ into irreducible polynomials:*

$$F(X,\alpha) = f_1(X) \cdots f_r(X).$$

Then for all but finitely many $\alpha \in \mathbb{Z}$ one can write $\alpha = \alpha_1 \cdots \alpha_r$ with α_i pairwise relatively prime such that

$$\left| \frac{\log|\alpha_i|}{\log|\alpha|} - \frac{\deg f_i}{\deg_X F} \right| < \epsilon.$$

In particular, when $\alpha = p^k$ is a prime power, this implies the Sprindžuk's irreducibility theorem. We are going to discuss only the latter, but the decomposition theorem is proved similarly. Later on we will give a more general statement of the decomposition theorem where α is a rational number, not an integer (see § 26).

We will use **heights**, which are a vital tool in Diophantine geometry. Now we make a long detour to define heights and establish their basic properties.

21 Heights on number fields

Informally, a "height" of an algebraic number is a measure of its complexity. We want it to satisfy the following properties.

(1) Height $H(\alpha)$ of an algebraic number $\alpha \in \overline{\mathbb{Q}}$ is a nonnegative real number.

(2) Heights behave well with respect to addition and multiplication. That is, $H(\alpha+\beta)$ and $H(\alpha\beta)$ can be reasonably estimated in terms of $H(\alpha)$ and $H(\beta)$.

(3) The **Northcott's property** (discreteness) holds: there are finitely many algebraic numbers of bounded height and bounded degree.

For $\alpha \in \mathbb{Z}$ taking $H(\alpha) := |\alpha|$, the usual absolute value, gives such a "height". However, on $\mathbb{Q}$ this does not satisfy the last property (3). For instance, the number $\frac{2014}{2013}$ is "complicated", but its absolute value is small. This suggests that on rational numbers a right notion of height is the following.

Definition 21.1. Let $\alpha \in \mathbb{Q}$ where $\alpha = \frac{a}{b}$ with $a, b \in \mathbb{Z}$ relatively prime. Then the **height** of α is given by $H(\alpha) := \max\{|\alpha|, |\beta|\}$.

In particular, for $\alpha \in \mathbb{Z}$ we have $H(\alpha) = \max\{|\alpha|, 1\}$.
This behaves well for products and sums, in the sense that there are bounds

$$H(\alpha\beta) \leq H(\alpha)\,H(\beta),$$
$$H(\alpha+\beta) \leq 2\,H(\alpha)\,H(\beta).$$

We want to extend the notion of height to algebraic numbers $\alpha \in \overline{\mathbb{Q}}$. The first idea that comes to mind is that for α one should consider its primitive minimal polynomial $f(X) \in \mathbb{Z}[X]$:

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0, \quad \text{where } (a_0, \ldots, a_n) = 1.$$

And one can put $\mathfrak{H}(\alpha) := \max\{|\alpha_0|, \dots, |\alpha_n|\}$. It is possible to study this height $\mathfrak{H}$ and show nontrivial results about it, however it is difficult to estimate $\mathfrak{H}(\alpha\beta)$ and $\mathfrak{H}(\alpha+\beta)$ in terms of $\mathfrak{H}(\alpha)$ and $\mathfrak{H}(\beta)$. So this idea is wrong (that is why it is "$\mathfrak{H}$" and not "H").

The second idea comes from the following observation: if $\alpha \in \mathbb{Q}$, then

$$H(\alpha) = \prod_{\nu \in M_{\mathbb{Q}}} \max\{1, |\alpha|_\nu\},$$

where $M_{\mathbb{Q}}$ are the usual absolute values (normalized by $|p|_p = 1/p$).

Example 21.2. For $\alpha = -\frac{12}{5}$ the absolute values are

$$|\alpha|_\nu = \begin{cases} \frac{1}{4}, & \nu = 2, \\ \frac{1}{3}, & \nu = 3, \\ 5, & \nu = 5, \\ \frac{12}{5}, & \nu = \infty, \\ 1, & \text{otherwise.} \end{cases}$$

Now $\prod_{\nu \in M_{\mathbb{Q}}} \max\{1, |\alpha|_\nu\} = 12$, which is the height of α. ▲

In general, for $\alpha = \frac{a}{b}$ one has

$$\prod_{\substack{\nu \in M_{\mathbb{Q}} \\ \nu \neq \infty}} \max\{1, |\alpha|_\nu\} = |b|.$$

And $\max\{1, |\alpha|_\infty\} = \max\{1, \frac{|a|}{|b|}\}$, so

$$\prod_{\nu \in M_{\mathbb{Q}}} \max\{1, |\alpha|_\nu\} = \max\{|b|, |a|\} = H(\alpha).$$

Now let K be a number field and M_K be the set of places on K. We assume that the places are normalized such that on $\mathbb{Q}$ they give the standard p-adic absolute values. Recall that for $\alpha \in \mathbb{Q}^\times$ one has the product formula

$$\prod_{\nu \in M_{\mathbb{Q}}} |\alpha|_\nu = 1.$$

For an arbitrary number field the product formula for $\alpha \in K^\times$ is

$$\prod_{\nu \in M_K} |\alpha|_\nu^{d_\nu} = 1, \quad \text{where } d_\nu := [K_\nu : \mathbb{Q}_\nu].$$

This can be immediately verified for $\alpha \in \mathbb{Q}^\times$. In this case for $p \in M_{\mathbb{Q}}$ one has several places $\nu \in M_K$ coming from p, and

$$\prod_{\substack{\nu \in M_K \\ \nu | p}} |\alpha|_\nu^{d_p} = |\alpha|_p^{\sum_{\nu|p} d_\nu} = |\alpha|_p^{[K:\mathbb{Q}]}.$$

So finally

$$\prod_{\nu \in M_K} |\alpha|_\nu^{d_\nu} = \left(\prod_{p \in M_{\mathbb{Q}}} |\alpha|_p \right)^{[K:\mathbb{Q}]} = 1$$

by the usual product formula for $\mathbb{Q}$.

In general for $\alpha \in K$ we have an embedding $K \hookrightarrow K_v$ and the corresponding absolute value is given by

$$|\alpha|_v := |N_{K_v/\mathbb{Q}_v}(\alpha)|_p^{1/d_v}.$$

So $|\alpha|_v^{d_v} = |N_{K_v/\mathbb{Q}_v}(\alpha)|_p$. We have

$$\prod_{v|p} |\alpha|_v^{d_v} = \prod_{v|p} |N_{K_v/\mathbb{Q}_v}(\alpha)|_p = |N_{K/\mathbb{Q}}(\alpha)|_p,$$

since the product of *local norms* $N_{K_v/\mathbb{Q}_v}$ gives the *global norm* $N_{K/\mathbb{Q}}$.

Thus everything reduces to the usual product formula for $\mathbb{Q}$:

$$\prod_{v \in M_K} |\alpha|_v^{d_v} = \prod_{p \in M_\mathbb{Q}} |N_{K/\mathbb{Q}}(\alpha)|_p = 1.$$

Remark 21.3. Sometimes one normalizes the absolute values by local degrees d_v putting $\|x\|_v := |x|_v^{d_v}$, so that the product formula reads $\prod_{v \in M_K} \|\alpha\|_v = 1$. We do not use this normalization, so be careful reading other books and articles.

Now the product formula for number fields suggests the following definition.

Definition 21.4. Let K be a fixed number field. The **height** of a number $\alpha \in K$ is

$$H_K(\alpha) := \prod_{v \in M_K} \max\{1, |\alpha|_v\}^{d_v}.$$

Taking logarithms, we get the **logarithmic height**

$$h_K(\alpha) := \sum_{v \in M_K} d_v \log^+ |\alpha|_v,$$

where $\log^+ x := \max\{0, \log x\}$. We assume $\log^+ 0 := 0$.

The whole point of taking logarithms is just that it is easier to write sums instead of products in various inequalities involving heights. In what follows we will mostly use "h" instead of "H".

The last definition of H_K and h_K depends on K, so we should correct it to define heights on the whole $\overline{\mathbb{Q}}$.

Proposition 21.5. *Let L/K be a finite extension and $\alpha \in K$. Then $h_L(\alpha) = [L:K] \cdot h_K(\alpha)$, and correspondingly $H_L(\alpha) = H_K(\alpha)^{[L:K]}$.*

Proof. Consider a place $w \in M_L$ coming from $v \in M_K$. We have $|\alpha|_w = |\alpha|_v$, and

$$d_w = [L_v : \mathbb{Q}_v] = [L_w : K_v] \cdot \underbrace{[K_v : \mathbb{Q}_v]}_{d_v}.$$

Now

$$\sum_{w|v} d_w \log^+ |\alpha|_w = \sum_{w|v} [L_w : K_v] \cdot d_v \log^+ |\alpha|_v = [L:K] \cdot d_v \log^+ |\alpha|_v,$$

since $\sum_{w|v} [L_w : K_v] = [L:K]$. And finally,

$$\sum_{w \in M_L} d_w \log^+ |\alpha|_w = [L:K] \cdot \sum_{v \in M_K} d_v \log^+ |\alpha|_v = [L:K] \cdot h_K(\alpha).$$

■

So the right definition of height is the following

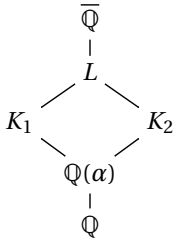
Definition 21.6. Let $\alpha \in \overline{\mathbb{Q}}$ be an algebraic number. Then its **height** (**logarithmic height**) is given by

$$H(\alpha) := H_K(\alpha)^{1/[K:\mathbb{Q}]},$$
$$h(\alpha) := \frac{1}{[K:\mathbb{Q}]} h_K(\alpha),$$

where K is some number field containing α.

The definition is correct thanks to the last proposition. Indeed, if $\alpha \in K_1$ and $\alpha \in K_2$, then there is L containing both K_1 and K_2 and

$$h_L(\alpha) = [L:K_1] \cdot h_{K_1}(\alpha) = [L:K_2] \cdot h_{K_2}(\alpha).$$



$$\frac{h_{K_1}(\alpha)}{[K_1:\mathbb{Q}]} = \frac{h_L(\alpha)}{[L:\mathbb{Q}]} = \frac{h_{K_2}(\alpha)}{[K_2:\mathbb{Q}]}.$$

So we finally have a right height function $h\colon \overline{\mathbb{Q}} \to \mathbb{R}_{\geq 0}$.

22 Projective and affine heights

Let K be a field. We have the affine space $\mathbb{A}^n(K)$ with coordinates $\{(\alpha_1,\dots,\alpha_n) \mid \alpha_i \in K\}$ and the projective space $\mathbb{P}^n(K)$ with projective coordinates $(\alpha_0 : \alpha_1 : \cdots : \alpha_n)$, where

$$(\alpha_0 : \alpha_1 : \cdots : \alpha_n) \sim (\lambda\alpha_0 : \lambda\alpha_1 : \cdots : \lambda\alpha_n) \quad \text{for } \lambda \in K^\times.$$

Definition 22.1. The **projective height** of a point $\underline{\alpha} = (\alpha_0 : \alpha_1 : \cdots : \alpha_n) \in \mathbb{P}^n(\overline{\mathbb{Q}})$ is given by

$$h_{\mathbb{P}}(\underline{\alpha}) := \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} d_v \log |\underline{\alpha}|_v,$$

where $|\underline{\alpha}|_v := \max\{|\alpha_0|_v,\dots,|\alpha_n|_v\}$, and K is some number field containing $\alpha_1,\dots,\alpha_n$.

(We write log instead of $\log^+$ since the point "$(0:0:\cdots:0)$" is not in $\mathbb{P}^n$.)

This does not depend on the field K and it is well-defined on $\mathbb{P}^n(\overline{\mathbb{Q}})$, i.e. $h_{\mathbb{P}}(\underline{\alpha}) = h_{\mathbb{P}}(\lambda\underline{\alpha})$ for $\lambda \in \overline{\mathbb{Q}}^\times$, since

$$h_{\mathbb{P}}(\lambda\underline{\alpha}) = h_{\mathbb{P}}(\underline{\alpha}) + \frac{1}{[K:\mathbb{Q}]} \underbrace{\sum_{v \in M_K} d_v \log |\lambda|_v}_{= \log \prod |\lambda|_v^{d_v} = 0}.$$

Definition 22.2. For a point $\underline{\alpha} = (\alpha_1,\dots,\alpha_n) \in \mathbb{A}^n(\overline{\mathbb{Q}})$ the **affine height** $h_{\mathbb{A}}$ is given via the embedding

$$\mathbb{A}^n(\overline{\mathbb{Q}}) \hookrightarrow \mathbb{P}^n(\overline{\mathbb{Q}}),$$
$$(\alpha_1,\dots,\alpha_n) \mapsto (1 : \alpha_1 : \cdots : \alpha_n).$$

In other words,

$$h_{\mathbb{A}}(\underline{\alpha}) = h_{\mathbb{P}}(1 : \alpha_1 : \cdots : \alpha_n) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} d_v \log^+ |\underline{\alpha}|_v.$$

Finally, we will need a notion of projective and affine height for a polynomial with coefficients in a number field.

Definition 22.3. For a polynomial $F(X_1, \ldots, X_n) = \sum_{i_i,\ldots,i_n} a_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n} \in K[X_1, \ldots, X_n]$ we put

$$h_{\mathbb{P}}(F) := h_{\mathbb{P}}(a_{i_1,\ldots,i_n})_{i_i,\ldots,i_n},$$
$$h_{\mathbb{A}}(F) := h_{\mathbb{A}}(a_{i_1,\ldots,i_n})_{i_i,\ldots,i_n}.$$

For $\lambda \in K^\times$ one has $h_{\mathbb{P}}(\lambda F) = h_{\mathbb{P}}(F)$. There is an inequality $h_{\mathbb{P}}(F) \le h_{\mathbb{A}}(F)$, and one has $h_{\mathbb{P}}(F) = h_{\mathbb{A}}(F)$ when one of the coefficients of F equals 1.

23 Properties of heights

Now we summarize and prove some basic properties of the height of an algebraic number $h(\alpha)$ defined above:

$$h(\alpha) := \frac{1}{[K:\mathbb{Q}]} h_K(\alpha) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} d_v \log^+ |\alpha|_v.$$

(1) $h(\alpha) \ge 0$ for any $\alpha \in \overline{\mathbb{Q}}$.

(2) $h(\alpha_1 \cdots \alpha_m) \le h(\alpha_1) + \cdots + h(\alpha_m)$.

(3) $h(\alpha_1 + \cdots + \alpha_m) \le h(\alpha_1) + \cdots + h(\alpha_m) + \log m$.

(4) $h(\alpha^n) = |n| \cdot h(\alpha)$. In particular, $h(\alpha^{-1}) = h(\alpha)$ for $\alpha \ne 0$.

(5) If α and β are conjugate over $\mathbb{Q}$, then $h(\alpha) = h(\beta)$.

(6) The **Northcott's property**: for fixed constant $C > 0$ and fixed degree $d = 1, 2, 3, \ldots$ the set

$$\{\alpha \mid h(\alpha) < C \text{ and } [\mathbb{Q}(\alpha) : \mathbb{Q}] < d\}$$

is finite.

(7) The **first Kronecker's theorem**: $h(\alpha) = 0$ iff $\alpha = 0$ or α is a root of unity.

We begin with the first, easier properties. The property (1) is obvious.

For the estimate (2), write

$$|\alpha_1 \cdots \alpha_m|_v = |\alpha_1|_v \cdots |\alpha_m|_v \le \max\{1, |\alpha_1|_v\} \cdots \max\{1, |\alpha_m|_v\}.$$

Taking logarithms, we get

$$\log^+ |\alpha_1 \cdots \alpha_m|_v \le \log^+ |\alpha_1|_v + \cdots + \log^+ |\alpha_m|_v,$$

which implies (2). ■

Similarly we show (3), but one should distinguish archimedian and nonarchimedian absolute values:

$$|\alpha_1+\cdots+\alpha_m|_v \le \left\{ \begin{array}{ll} \max\{|\alpha_1|_v,\ldots,|\alpha_m|_v\}, & v \text{ nonarchimedian} \\ m\cdot\max\{|\alpha_1|_v,\ldots,|\alpha_m|_v\}, & v \text{ archimedian} \end{array} \right\}$$

$$\le \left\{ \begin{array}{ll} \max\{1,|\alpha_1|_v\}\cdots\max\{1,|\alpha_m|_v\}, & v \text{ nonarchimedian} \\ m\cdot\max\{1,|\alpha_1|_v\}\cdots\max\{1,|\alpha_m|_v\}, & v \text{ archimedian} \end{array} \right\}$$

Taking logarithms,

$$\log^+|\alpha_1+\cdots+\alpha_m| \le \log^+|\alpha_1|+\cdots+\log^+|\alpha_m|+\left\{ \begin{array}{ll} 0, & v \text{ nonarchimedian} \\ \log m, & v \text{ archimedian} \end{array} \right\}$$

Thus

$$h(\alpha_1+\cdots+\alpha_m) \le h(\alpha_1)+\cdots+h(\alpha_m)+\frac{1}{[K:\mathbb{Q}]}\sum_{v|\infty} d_v \log m = h(\alpha_1)+\cdots+h(\alpha_m)+\log m,$$

since $\sum_{v|\infty} d_v = [K:\mathbb{Q}]$. ■

Now for (4) observe that $h(\alpha^n) = |n|\cdot h(\alpha)$ for $n>0$ since $\max\{1,|\alpha^n|_v\} = \max\{1,|\alpha|_v\}^n$.
The key case is (4) for $n=-1$. We have $\log^+|\alpha^{-1}|_v = -\log^-|\alpha|_v$ where $\log^- x := \min\{0,\log x\}$. Now

$$h(\alpha^{-1})-h(\alpha) = \frac{1}{[K:\mathbb{Q}]}\left(\sum_{v\in M_K} d_v \log^+|\alpha|_v + \sum_{v\in M_K}\log^-|\alpha|_v\right) = \frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K} d_v \log|\alpha|_v = 0$$

by the product formula.
If $n<-1$, then from what we have proved, $h(\alpha^{-n}) = h((\alpha^{-1})^n) = |n|\cdot h(\alpha^{-1}) = |n|\cdot h(\alpha)$. ■

Now we show (5). Suppose α and β are conjugate. That is, let $K/\mathbb{Q}$ be a Galois extension containing both α and β and let $\sigma\in \mathrm{Gal}(K/\mathbb{Q})$ be such that $\sigma(\alpha)=\beta$.
The Galois group $\mathrm{Gal}(K/\mathbb{Q})$ acts on the set of places M_K. Each $\sigma\in\mathrm{Gal}(K/\mathbb{Q})$ induces a permutation

$$\begin{aligned} M_K &\to M_K, \\ v &\mapsto v^\sigma, \end{aligned}$$

where we define $|x|_{v^\sigma} := |\sigma(x)|_v$. On $\mathbb{Q}$ the absolute value $|\cdot|_{v^\sigma}$ coincides with $|\cdot|_v$. The inverse map is given by $v\mapsto v^{\sigma^{-1}}$. We have

$$h(\beta) = \frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K} d_v \log^+|\beta|_v = \frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K} d_v \log^+|\alpha|_{v^\sigma} = \frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K} d_v \log^+|\alpha|_v = h(\alpha),$$

using the fact that $\mathrm{Gal}(K/\mathbb{Q})$ just permutes the places, and that $d_v = d_{v^\sigma}$. ■

Example 23.1. Consider $K=\mathbb{Q}(\gamma)$ where γ is a root of X^2-2. There are two real embeddings of K, and so there are two extensions of $|\cdot|_\infty$ from $\mathbb{Q}$ to K:

$$\begin{aligned} K &\hookrightarrow \mathbb{R}, \\ v_+ &: \gamma \mapsto +\sqrt{2}, \\ v_- &: \gamma \mapsto -\sqrt{2}. \end{aligned}$$

Consider two conjugate numbers $\alpha = 1+\gamma$ and $\beta = 1-\gamma$. One has

$$h(\alpha) = \frac{1}{2}\left(\log^+|\alpha|_{v^+} + \log^+|\alpha|_{v^-}\right) = \frac{1}{2}\left(\log^+|1+\sqrt{2}| + \underbrace{\log^+|1-\sqrt{2}|}_{=0}\right) = \frac{1}{2}\log|1+\sqrt{2}|.$$

$$h(\beta) = \frac{1}{2}\left(\log^+|\beta|_{v^+} + \log^+|\beta|_{v^-}\right) = \frac{1}{2}\left(\underbrace{\log^+|1-\sqrt{2}|}_{=0} + \log^+|1+\sqrt{2}|\right) = \frac{1}{2}\log|1+\sqrt{2}|.$$

▲

Now we are going to show the Northcott's property (6). For this it is enough to show that for a fixed $C > 0$ and a fixed degree d the set

$$A := \{\alpha \in \overline{\mathbb{Q}} \mid h(\alpha) < C,\ [\mathbb{Q}(\alpha) : \mathbb{Q}] = d\}$$

is finite. We already know that this is the case when $d = 1$.

Let $\alpha \in A$. Consider the minimal polynomial $f(X) \in \mathbb{Q}[X]$ of α:

$$f(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_1 X + a_0.$$

Let $\alpha_1 = \alpha, \ldots, \alpha_d$ be the conjugates of α (that is, the roots of f) and write down the Vieta's formulas:

$$\begin{aligned}
a_0 &= (-1)^d\,\alpha_1\,\alpha_2\cdots\alpha_d,\\
a_1 &= (-1)^{d-1}\,(\alpha_1\,\alpha_2\cdots\alpha_{d-1} + \alpha_1\,\alpha_2\cdots\alpha_{d-2}\,\alpha_d + \ldots + \alpha_2\,\alpha_3\cdots\alpha_d),\\
&\vdots\\
a_{d-3} &= -(\alpha_1\,\alpha_2\,\alpha_3 + \alpha_1\,\alpha_2\,\alpha_4 + \cdots + \alpha_{d-2}\,\alpha_{d-1}\,\alpha_d),\\
a_{d-2} &= \alpha_1\,\alpha_2 + \alpha_1\,\alpha_3 + \cdots + \alpha_1\,\alpha_d + \alpha_2\,\alpha_3 + \cdots + \alpha_{d-1}\,\alpha_d,\\
a_{d-1} &= -(\alpha_1 + \alpha_2 + \cdots + \alpha_d).
\end{aligned}$$

Since $\alpha_1, \ldots, \alpha_d$ are conjugate, we have

$$h(\alpha_1) = h(\alpha_2) = \cdots = h(\alpha_d) < C,$$

and from these identities and the properties (2) and (3)

$$\begin{aligned}
h(a_0) &\le C^d,\\
h(a_1) &\le d\,C^{d-1} + \log d,\\
&\vdots\\
h(a_{d-3}) &\le \binom{d}{3} C^3 + \log\binom{d}{3},\\
h(a_{d-2}) &\le \binom{d}{2} C^2 + \log\binom{d}{2},\\
h(a_{d-1}) &\le d\,C + \log d.
\end{aligned}$$

Thus the heights of the coefficients $a_0, a_1, \ldots, a_{d-1} \in \mathbb{Q}$ are bounded in terms of C and d, which means there are finitely many choices for $a_0, \ldots, a_d$, hence finitely many choices for $f(X)$ and finitely many choices for α. ■

Finally we show the first Kronecker's theorem (7). If $\alpha = 0$, then $h(\alpha) = 0$. If $\alpha^n = 1$ for some n, then

$$0 = h(1) = h(\alpha^n) = |n| \cdot h(\alpha).$$

In the other direction, assume that $h(\alpha^n) = 0$ for some n. Consider the numbers $1, \alpha, \alpha^2, \alpha^3, \ldots$ Their degree $[\mathbb{Q}(\alpha^k) : \mathbb{Q}]$ is bounded by $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$ and their height is bounded since $h(\alpha^n) = 0$. So in this sequence there are finitely many numbers, and there are some k and ℓ such that $\alpha^k = \alpha^\ell$, which implies that $\alpha = 0$ or α is a root of unity. ■

We are done with proving the properties (1)–(7) and now we discuss some related results. There is also the **second Kronecker's theorem**, related to the first theorem.

Theorem 23.2 (Second Kronecker's theorem)**.** *For each d there exists a constant $C(d) > 0$, such that for any $\alpha \in \overline{\mathbb{Q}}^\times$ which is not a root of unity, $[\mathbb{Q}(\alpha) : \mathbb{Q}] \le d$ implies $h(\alpha) \ge C(d)$.*

Proof. Consider the set

$$A := \{\beta \in \overline{\mathbb{Q}} \mid [\mathbb{Q}(\beta) : \mathbb{Q}] \le d,\ h(\beta) \le 1\}.$$

This is a finite set, having $\Theta_d := |A|$ elements. Consider a sequence

$$1, \alpha, \alpha^2, \ldots, \alpha^{\Theta_d}.$$

These numbers are pairwise distinct, since $\alpha \neq 0$ and α is not a root of unity by our assumption. But there are $\Theta_d + 1$ numbers, so there is some $k \le \Theta_d$ such that $\alpha^k \notin A$, so that $h(\alpha^k) > 1$ and $h(\alpha) > \frac{1}{k} \ge \frac{1}{\Theta_d}$. Now put $C(d) := \frac{1}{\Theta_d}$ and we are done. ■

The estimate for $C(d)$ produced in the proof above is very poor. The **Lehmer's conjecture** states that $C(d) = \frac{C}{d}$ where C is some universal constant. The smallest known candidate to be C is the largest real root of a polynomial

$$X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1.$$

This root is $\approx 1.176280818\ldots$ A special feature of this example is that the minimal polynomial of α, which is given above, is palindromic. An algebraic number α is called **reciprocal** if α and α^{-1} are conjugate over $\mathbb{Q}$ (which means the minimal polynomial of α is palindromic). One result towards the Lehmer's conjecture is the following:

Theorem 23.3 (Chris Smyth, 1971)**.** *If α is nonreciprocal and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$, then $h(\alpha) \ge \log\theta / d$ where $\theta \approx 1.324717957\ldots$ is the real root of $X^3 - X - 1$, and it is the best possible estimate (for nonreciprocal numbers).*

As for reciprocal numbers, the conjecture still remains open, and the best know result is due to Dobrowolski (1978):

$$h(\alpha) \ge \frac{C}{d}\left(\frac{\log\log d}{\log d}\right)^3.$$

In some practical applications one can neglect the multiplier $\left(\frac{\log\log d}{\log d}\right)^3$, although it seems to be difficult to remove it or at least improve.

Let $\alpha \in \mathbb{Q}^\times$ be a rational number $\alpha = \frac{a}{b}$ with $(a, b) = 1$. Then $|\alpha| \ge \frac{1}{b}$ and $b \le H(\alpha) = e^{h(\alpha)}$. So we have the so-called **Liouville's inequality**

$$|\alpha| \ge e^{-h(\alpha)}.$$

This easy observation generalizes to any number field K and any absolute value $|\cdot|_v$.

Proposition 23.4. *Let K be a number field. Let $v \in M_K$. Then for $\alpha \in K$ one has*

$$|\alpha|_v^{d_v} \ge e^{-[K:\mathbb{Q}]\cdot h(\alpha)}.$$

More generally, for a set of places $S \subset M_K$ one has

$$\prod_{v \in S} |\alpha|_v^{d_v} \ge e^{-[K:\mathbb{Q}]\cdot h(\alpha)}.$$

Proof. We have the product formula

$$\prod_{v\in M_K} |\alpha|_v^{d_v} = 1.$$

So if we take a product outside some subset $S \subset M_K$, there is an inequality

$$\prod_{v\in M_K\setminus S} |\alpha|_v^{d_v} \le \prod_{v\in M_K\setminus S} \max\{1,|\alpha|_v\}^{d_v} \le \prod_{v\in M_K} \max\{1,|\alpha|_v\}^{d_v} = H_K(\alpha) = e^{[K:\mathbb{Q}]\cdot h(\alpha)}.$$

Now

$$\prod_{v\in S} |\alpha|_v^{d_v} = \left(\prod_{v\in M_K\setminus S} |\alpha|_v^{d_v}\right)^{-1} \ge e^{-[K:\mathbb{Q}]\cdot h(\alpha)}.$$

■

Finally, we want to show a relationship between the height $h(\alpha)$ of an algebraic number $\alpha \in \overline{\mathbb{Q}}$ and the height of a polynomial $f \in \overline{\mathbb{Q}}[X]$ having α as its root; and also with the heights of the values of the polynomial.

Lemma 23.5. *Let $f(X) = a_nX^n + \cdots + a_1X + a_0 \in K[X]$ be a polynomial and $|\cdot|_v$ be an absolute value on K. Set $|f|_v := \max\{|a_0|_v,\ldots,|a_n|_v\}$. Let α be a root of $f(X)$. Then*

$$|\alpha|_v \le \begin{cases} \frac{|f|_v}{|a_n|_v}, & v \text{ nonarchimedian,} \\ 2\frac{|f|_v}{|a_n|_v}, & v \text{ archimedian.} \end{cases}$$

Proof. To simplify the notation, we write just $|\cdot|$ instead of $|\cdot|_v$.

Since $|f|$ is by definition the maximum of $|a_i|$, we have $\frac{|f|}{|a_n|} \ge 1$. If $|\alpha| < 1$, then

$$|\alpha| < \frac{|f|}{|a_n|} \le 2\,\frac{|f|}{|a_n|},$$

and we are done.

Now for $|\alpha| \ge 1$ we consider the expression

$$\alpha^n = -\sum_{0\le i\le n-1} \frac{a_i}{a_n}\alpha^i.$$

We take the absolute values $|\cdot|$ and estimate the right hand side. In the nonarchimedian case

$$|\alpha|^n = \left|\sum_{0\le i\le n-1} \frac{a_i}{a_n}\,\alpha^i\right| \le \frac{|f|}{|a_n|}\,|\alpha|^{n-1},$$

thus $|\alpha| \le \frac{|f|}{|a_n|}$. (In the bound we indeed used that $|\alpha| \ge 1$.)

In the archimedian case we do the same estimates, but we have to use the triangle inequality. Observe that we can assume $|\alpha| > 2$, otherwise the claimed inequality is trivially true.

$$\begin{aligned} |\alpha|^n = \left|\sum_{0\le i\le n-1} \frac{a_i}{a_n}\,\alpha^i\right| &\le \sum_{0\le i\le n-1} \frac{|a_i|}{|a_n|}\,|\alpha|^i \\ &= |\alpha^{n-1}|\sum_{0\le i\le n-1} \frac{|a_i|}{|a_n|}\,|\alpha|^{i-(n-1)} \\ &\le |\alpha^{n-1}|\,\frac{|f|}{|a_n|}\left(1+\frac{1}{|\alpha|}+\frac{1}{|\alpha|^2}+\cdots+\frac{1}{|\alpha|^{n-1}}\right) \\ &\le |\alpha^{n-1}|\,\frac{|f|}{|a_n|}\left(1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots\right) \\ &\le 2\,|\alpha^{n-1}|\,\frac{|f|}{|a_n|}. \end{aligned}$$

(Note the interesting trick we used; a simple-minded application of the triangle inequality gives immediately $|\alpha| \leq n\frac{|f|}{|a_n|}$, but we were able to replace "n" with "2".) ■

Proposition 23.6. *Let $f(X) \in \overline{\mathbb{Q}}[X]$ be a nonzero polynomial and $\alpha \in \overline{\mathbb{Q}}$ be its root. Then $h(\alpha) \leq h_{\mathbb{P}}(f) + \log 2$.*

Proof. Let $f(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$. We have

$$|\alpha|_v \leq \begin{cases} \frac{|f|_v}{|a_n|_v}, & v \text{ nonarchimedian,} \\ 2\frac{|f|_v}{|a_n|_v}, & v \text{ archimedian.} \end{cases}$$

Thus

$$\log^+ |\alpha|_v \leq \log \frac{|f|_v}{|a_n|_v} + \left\{ \begin{array}{ll} 0, & v \text{ nonarchimedian,} \\ \log 2, & v \text{ archimedian.} \end{array} \right\}$$

And so

$$h(\alpha) \leq h_{\mathbb{P}}\left(\frac{f}{a_n}\right) + \log 2 = h_{\mathbb{P}}(f) + \log 2.$$

■

Remark 23.7. A stronger estimate can be proven. If $\alpha_1, \ldots, \alpha_n$ are all roots of f then

$$\left| h_{\mathbb{P}}(f) - \sum_{1 \leq i \leq n} h(\alpha_i) \right| \leq c(n).$$

For some constant $c(n)$ depending on n.

Proposition 23.8. *Let $f(X) \in \overline{\mathbb{Q}}[X]$ be a nonzero polynomial of degree m and let $\alpha \in \overline{\mathbb{Q}}$. Then*

$$h(f(\alpha)) \leq m\, h(\alpha) + h_{\mathbb{A}}(f) + \log(m+1).$$

Proof. Let $f(X) = a_m X^m + a_{m-1}X^{m-1} + \cdots + a_1 X + a_0$. We have

$$|f(\alpha)|_v \leq \max\{|a_0|_v, \ldots, |a_m|_v\} \cdot \left\{ \begin{array}{ll} 1, & v \text{ nonarchimedian,} \\ m+1, & v \text{ archimedian.} \end{array} \right\}$$

So

$$\max\{1, |f(\alpha)|_v\} \leq \max\{1, |a_0|_v, \ldots, |a_m|_v\} \cdot \left\{ \begin{array}{ll} 1, & v \text{ nonarchimedian,} \\ m+1, & v \text{ archimedian.} \end{array} \right\}$$

$$h(f(\alpha)) \leq h_{\mathbb{A}}(f) + m\, h(\alpha) + \log(m+1).$$

■

Similarly one can show the following:

Proposition 23.9. *Let $F(X,T) \in \overline{\mathbb{Q}}[X,T]$ be a polynomial of degrees $\deg_X F = n$, $\deg_T F = m$. Let $\alpha, \beta \in \overline{\mathbb{Q}}$. Then*

$$h(F(\beta,\alpha)) \leq m\, h(\beta) + n\, h(\alpha) + h_{\mathbb{A}}(F) + \log((m+1)\cdot(n+1)).$$

Finally, we show another bound for polynomials in two variables.

Proposition 23.10. *Let $F(X,T) \in \overline{\mathbb{Q}}[X,T]$ be a polynomial of degrees $\deg_T F = m$, $\deg_X F = n$. Let $\alpha, \beta \in \overline{\mathbb{Q}}$ be such that $F(\beta,\alpha) = 0$ and $F(X,\alpha)$ is not identically zero. Then*

$$h(\beta) \leq m\, h(\alpha) + h_{\mathbb{P}}(F) + \log 2\,(m+1).$$

Proof. Put $f(X) := F(X, \alpha)$. It is a polynomial in one variable having β as its root. So $h(\beta) \le h_{\mathbb{P}}(f) + \log 2$ by proposition 23.6. It remains to show a bound on $h_{\mathbb{P}}(f)$.

Let $F(X,T) = g_n(T)\,X^n + \cdots + g_1(T)\,X + g_0(T)$ for some $g_0, \dots, g_n \in \overline{\mathbb{Q}}[T]$. Then $f(X) = g_n(\alpha)\,X^n + \cdots + g_1(\alpha)\,X + g_0(\alpha)$. Let K be a number field containing α and let $v \in M_K$ be a place on K. Consider $g_i(T) = a_m\,T^m + \cdots + a_1\,T + a_0$ one of the polynomials $g_0, \dots, g_n$.

$$|g(\alpha)|_v \le \max\{1, |\alpha|_v\}^m \cdot |g|_v \cdot \left\{ \begin{array}{ll} 1, & v \text{ nonarchimedian,} \\ m+1, & v \text{ archimedian.} \end{array} \right\}$$

Since $|g|_v \le |F|_v$, we get

$$h_{\mathbb{P}}(f) \le \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_k} d_v \log^+ |f|_v \le m\,h(\alpha) + h_{\mathbb{P}}(F) + \log(m+1).$$

Now substituting this in the bound $h(\beta) \le h_{\mathbb{P}}(f) + \log 2$, we get the desired result. ■

Remark 23.11. The proposition above does not give the optimal bound. One can show that

$$\frac{h(\alpha)}{n} \approx \frac{h(\beta)}{m},$$

where $m = \deg_T F$, $n = \deg_X F$, and $\approx$ is a "quasi-equivalence of heights" (the difference of heights is "small"; we omit the details).

24 Eisenstein theorem about algebraic power series

Let $x(T) \in \overline{\mathbb{Q}}[[T]]$ be a formal power series

$$x(T) = a_0 + a_1\,T + a_2\,T^2 + \cdots, \quad a_i \in \overline{\mathbb{Q}}.$$

We say that $x(T)$ is **algebraic** if it is algebraic over $\mathbb{Q}(T)$; that is, there is some polynomial $F(X,T) \in \overline{\mathbb{Q}}[X,T]$ such that $F(x(T),T) = 0$ in the ring $\overline{\mathbb{Q}}[[T]]$:

$$F(x(T),T) = g_0(T) + g_1(T)\,x(T) + \cdots + g_{N-1}(T)\,x^{N-1}(T) + g_N(T)\,x^N(T) = 0, \quad \text{for some } g_i(T) \in \overline{\mathbb{Q}}[T].$$

If $x(T)$ is an algebraic power series, then it lies in a finite extension of $\mathbb{Q}((T))$, so the residue field of $\mathbb{Q}((T))\,(x(T))$ is finite over $\mathbb{Q}$. This means that the coefficients a_i belong to some number field K.

Example 24.1. $x(T) = 1 + \sqrt{2}\,T + \sqrt{3}\,T^2 + \sqrt{4}\,T^3 + \cdots$ is not an algebraic power series, since the coefficients do not lie in a finite extension of $\mathbb{Q}$. ▲

Example 24.2. Consider a power series

$$x(T) = \frac{1}{2-T} = \frac{1}{2} \cdot \frac{1}{1 - T/2} = \frac{1}{2} \sum_{k \ge 0} \frac{T^k}{2^k}.$$

This is not just algebraic, but rational. In the denominators we have powers of 2. ▲

Example 24.3. Now consider a power series

$$x(T) = (1+T)^{1/2} = \sum_{k \ge 0} \binom{1/2}{k} T^k.$$

Compute the binomial coefficients

$$\binom{1/2}{k} := \frac{\frac{1}{2}\cdot(\frac{1}{2}-1)\cdot(\frac{1}{2}-2)\cdots(\frac{1}{2}-k+1)}{k!}.$$

k:	0	1	2	3	4	5	6	7	8	9	$\cdots$
$\binom{1/2}{k}$:	1	$+\frac{1}{2}$	$-\frac{1}{2^3}$	$+\frac{1}{2^4}$	$-\frac{5}{2^7}$	$+\frac{7}{2^8}$	$-\frac{21}{2^{10}}$	$+\frac{33}{2^{11}}$	$-\frac{429}{2^{15}}$	$+\frac{715}{2^{16}}$	$\cdots$

The key observation one makes from looking at the denominators is that $4^k \cdot \binom{1/2}{k}$ is always an integer (try to prove this). This is a general property of algebraic power series. ▲

Theorem 24.4 (Eisenstein)**.** *Let $x(T) = \sum_{k\geq 0} a_k T^k$ be an algebraic power series with $a_i \in K$. Then there exists an integer $c \in O_K$ such that $c^k a_k \in O_K$.*

This means that the denominators in an algebraic power series must have a very special "exponential" form.

Example 24.5. Consider the logarithm power series

$$\log(1+T) = \sum_{k\geq 1} (-1)^{k-1} \frac{T^k}{k}.$$

The denominators are not powers of some integer, so it is not an *algebraic* power series. Similarly the exponent

$$\exp(T) = \sum_{k\geq 0} \frac{T^k}{k!}$$

is not an algebraic power series. ▲

Let us give another statement of theorem 24.4. It says that for any nonarchimedian place $v \in M_K$ one has $|a_k|_v \leq (|c|_v^{-1})^k$. So the following holds:

Theorem 24.6 (Esenstein-2)**.** *Let $x(T) = \sum_{k\geq 0} a_k T^k$ be an algebraic power series with $a_i \in K$. Then for any place $v \in M_K$ there exists a number $A_v \in \mathbb{R}$, $A_v \geq 1$, such that $|a_k|_v \leq A_v^k$, and $A_v = 1$ for all but finitely many v.*

Remark 24.7. To see why theorem 24.6 is equivalent to theorem 24.4, recall what are the absolute values on a number field. For every $x \in K$ we can look at the *fractional* ideal factorization

$$xO_K = \prod_{\substack{\mathfrak{p}\subset O_K \\ \text{nonzero prime}}} \mathfrak{p}^{\nu_\mathfrak{p}(x)},$$

and by definition the number $\nu_\mathfrak{p}(x) \in \mathbb{Z}$ is the *valuation* of x at $\mathfrak{p}$. It defines in turn an absolute value $|x|_\mathfrak{p} := \rho^{\nu_\mathfrak{p}(x)}$. Any nonarchimedian absolute value on K is equivalent to some $|\cdot|_\mathfrak{p}$ (and the archimedian absolute values come from embeddings $K \hookrightarrow \mathbb{C}$, as we saw in § 17).

Further,

$$O_{K,\mathfrak{p}} = \{x \in K \mid |x|_\mathfrak{p} \leq 1\},$$

$$O_K = \bigcap_{\substack{\mathfrak{p}\subset O_K \\ \text{nonzero prime}}} O_{K,\mathfrak{p}} = \{x \in K \mid |x|_\mathfrak{p} \leq 1 \text{ for all } \mathfrak{p} \subseteq O_K\}.$$

Thus, assuming that $|a_k|_v \leq 1$ for all but finitely many finite places $v \in M_K$ and $|a_k|_v \leq A_v^k$ for *finitely many* v, we can find $c \in O_K$ with small enough absolute values with respect to each of these v (take a product of big powers of corresponding primes):

$$|c|_v \leq \frac{1}{A_v} \quad \text{so that} \quad |c^k a_k|_v = |c|_v^k \cdot |a_k|_v \leq 1.$$

Note that if the place $v \in M_K$ is infinite, then we can consider $x(T)$ as an analytic function. It is regular at 0 (having no poles and no ramifications), so it converges in some disk centered at 0. This means that the absolute values $|a_k|_v$ grow at most exponentially. So in the statement above by "any place $v \in M_K$" we really mean archimedian places as well.

Corollary 24.8. *For each v the power series $x(T)$ converges v-adically in* some *disk, and for all but finitely many v it converges in the unit disk.*

Observe that while the Eisenstein theorem implies this convergence property, there is no implication the other way round: for instance, the logarithm converges, but it contradicts the Eisenstein theorem.

25 Proof of the Sprindžuk's theorem

Now we go back to the Sprindžuk's theorem to prove it. Recall that for $\alpha \in \mathbb{Q}^\times$ we defined the set $S_\alpha := \{v \in M_\mathbb{Q} \mid |\alpha|_v < 1\}$ and

$$\Omega := \{p^k \mid p \text{ is prime},\ k = 1,2,3,\ldots\} \cup \{\frac{1}{n} \mid n \in \mathbb{Z} \setminus \{0\}\} \subset \{\alpha \in \mathbb{Q}^\times \mid |S_\alpha| = 1\}.$$

Let $F(X,T) \in \mathbb{Q}[X,T]$ be an irreducible polynomial over $\mathbb{Q}$ satisfying $F(0,0) = 0$ and $F'_X(0,0) \neq 0$. Then we want to conclude that for all but finitely many $\alpha \in \Omega$ the polynomial $F(X,\alpha) \in \mathbb{Q}[X]$ is irreducible over $\mathbb{Q}$.

Claim. *There exists a unique power series $x(T) \in \mathbb{Q}[[T]]$ such that $x(0) = 0$ (there is no free term) and $F(x(T),T) = 0$.*

This actually follows from the Hensel's lemma. We apply it to a polynomial $f(X) := F(X,T) \in \mathbb{Q}[[T]][X]$ with coefficients in a complete ring $\mathbb{Q}[[T]]$. One has $f(0) \equiv 0 \pmod{(T)}$ since $F(0,0) = 0$, and $f'(0) \not\equiv 0 \pmod{(T)}$ since $F'_X(0,0) \neq 0$. So the conditions of the Hensel's lemma are satisfied, and there is unique $x(T) \in \mathbb{Q}[[T]]$, as we want.

To this power series $x(T) = a_1 T + a_2 T^2 + a_3 T^3 + \cdots$ we apply the Eisenstein's theorem: for any place $v \in M_\mathbb{Q}$ there exists a number $A_v \geq 1$ (and $A_v = 1$ for all but finitely many v) such that $|a_k|_v \leq A_v^k$.

Claim. *At all but finitely many $T = \alpha \in \Omega$ the series $x(T)$ absolutely converges v-adically for $v \in S_\alpha$.*

Proof. $x(\alpha) = \sum_{k\geq 0} a_k \alpha^k$ converges whenever $|\alpha|_v < \frac{1}{A_v}$:

$$|a_k \alpha^k|_v = |a_k|_v \cdot |\alpha|_v^k \leq A_v^k \cdot |\alpha|_v^k < (A_v \cdot |\alpha|_v)^k \xrightarrow{k\to\infty} 0.$$

Assume that $|\alpha|_v \geq \frac{1}{A_v}$. Then we can bound the height of α by

$$h(\alpha) = h(\alpha^{-1}) = \sum_{v \in M_K} \log^+ |\alpha|_v^{-1} \leq \sum_{v \in M_K} \log^+ A_v.$$

Now for all but finitely many $v \in M_K$ one has $A_v = 1$, so the sum on the right hand side is finite. Moreover, the numbers A_v depend only on the polynomial $F(X,T)$ and not on α, so by the Northcott's property there are only finitely many α such that $|\alpha|_v \geq A_v$. ∎

Let β denote the v-adic sum of $x(T)$ at $T = \alpha$ for $v \in S_\alpha$. Since $F(x(T),T) = 0$, we get $F(\beta,\alpha) = 0$ (using the absolute convergence), so β is a root of $F(X,\alpha)$, and it is actually an algebraic number. We may assume $\deg_X F(X,\alpha) = \deg_X F = n$—this degree goes down when α satisfies some algebraic equations, so it is enough to disregard finitely many α. Now $F(X,\alpha)$ is irreducible over $\mathbb{Q}$ iff $[\mathbb{Q}(\beta) : \mathbb{Q}] = n$.

So for $K := \mathbb{Q}(\beta)$ we look at the degree $d := [K : \mathbb{Q}]$. We will show that $d = n$ for all but finitely many α, and it will establish the Sprindžuk's theorem.

The idea is to construct an **auxiliary polynomial** $G(X,T) \in \mathbb{Q}[X,T]$ such that $\gamma = G(\beta,\alpha)$ is "very small" v-adically. More precisely, we want the following properties:

- $G(X,T)$ is not identically 0.

- $\deg_X G \le n-1$, where $n := \deg_X F$.
- $\deg_T G \le N$, where N is some fixed big integer (later on we will set it), much bigger than m and n.
- $G(x(T),T)$ has a high order zero at 0.

The coefficients of $G(x(T),T)$ are linear combinations of coefficients of G, so vanishing of $G(x(T),T)$ at 0 of order μ is equivalent to μ linear equations imposed on the coefficients of G.

To find G with order of vanishing at least μ, we must have $\mu < n(N+1)$, where N is the maximal degree of g_i's in

$$G(X,T) = g_{n-1}(T)\,X^{n-1} + \cdots + g_1(T)\,X + g_0(T).$$

So each g_i gives $N+1$ coefficients.

To simplify the formulas, we may take $\mu = N\,n$. So by "vanishing of high order" we will mean order at least $N\,n$:

$$G(x(T),T) = y(T) = b_{N\,n}\,t^{N\,n} + \text{higher order terms}.$$

Let $\gamma := G(\beta,\alpha)$ be the v-adic sum of $y(T)$ at $T=\alpha$. For all but finitely many α we have $\gamma \neq 0$. Indeed, if $\gamma = 0$, then $F(\beta,\alpha) = 0$ and $G(\beta,\alpha) = 0$. But these two polynomials have no common factor in $\mathbb{Q}[X,T]$, and so they have only finitely many common roots (F is irreducible by our assumption, and $F \nmid G$ since $\deg_X G \le n-1$ and $\deg_X F = n$).

Proposition 25.1 (Baby algebraic geometry)**.** *Let K be a field. Let $F(X,T), G(X,T) \in K[X,T]$ be two polynomials. Assume that F and G have no common factor. Then the system of equations $F(x,t) = G(x,t) = 0$ has only finitely many solutions in $(x,t) \in K^2$.*

Now by Eisenstein's theorem, for all $v \in M_{\mathbb{Q}}$ there exists $B_v \ge 1$ (and $B_v = 1$ for all but finitely many v) such that $|b_k|_v \le B_v^k$. If v is nonarchimedian and $B_v = 1$, then $|b_k|_v \le 1$ and

$$|y(\alpha)|_v \le |\alpha|_v^{N\,n}.$$

If v is nonarchimedian and $B_v > 1$, then we may assume $|\alpha|_v < B_v^{-1}$ by disposing finitely many α (by the Northcott's property as above). After that one has

$$|b_k\,\alpha^k|_v \le (B_v \cdot |\alpha|_v)^k \le (B_v \cdot |\alpha|_v)^{N\,n} \le C \cdot |\alpha|_v^{N\,n},$$

where C is some constant depending on F and G, but not on α.

If v is archimedian, then we may assume $|\alpha|_v < (2\,B_v)^{-1}$.

$$|b_k\,\alpha^k|_v \le (B_v \cdot |\alpha|_v)^k \le \frac{1}{2}.$$

$$|y(\alpha)|_v \le \sum_{k \ge nN} (B_v \cdot |\alpha|_v)^k = (B_v \cdot |\alpha|_v)^{N\,n}\,\frac{1}{1 - B_v \cdot |\alpha|_v} \le 2\,(B_v \cdot |\alpha|_v)^{N\,n} \le C_v \cdot |\alpha|_v^{N\,n}.$$

Here $C_v = 1$ for all but finitely many v and it is some constant depending on F and G. So we have an upper bound for $\gamma := G(\beta,\alpha)$ β (proposition 23.9):

$$|\gamma|_v \le C_v \cdot |\alpha|_v^{N\,n}.$$

We have also a lower bound given by the Liouville's inequality

$$|\gamma|_v \ge e^{-d\,h(\gamma)}.$$

We want to get a contradiction from $e^{-d\,h(\gamma)} \le |\gamma|_v \le C_v \cdot |\alpha|_v^{N\,n}$. For this we write $h(\gamma)$ in terms of α. We use the bound

$$h(\gamma) \le h(\alpha)\,N + h(\beta)\,(n+1) + C,$$

where C is a constant depending only on G. The upper bound $|\gamma|_v \le C_v \cdot |\alpha|_v^{N\,n}$ can be written as $|\gamma|_v \le C\,e^{-N\,n\,h(\alpha)}$ where C is a constant depending on F and G. If we forget for a while about the term "$h(\beta)\,(n+1)$" above, then the bounds indeed give a contradiction if $d < n$:

$$e^{-d\,N\,h(\alpha)} < C\,e^{-n\,N\,h(\alpha)}.$$

Now we take care of the term "$h(\beta)\,(n+1)$". Since $F(\alpha,\beta) = 0$, we have $h(\beta) \le m\,h(\alpha) + O_\beta(1)$, where $O_\beta(1)$ is something does not depending on β (proposition 23.10). Now

$$h(\gamma) \le (N + m\,(n-1))\,h(\alpha) + C,$$

where C is a constant depending only on F and G.

So we get

$$|\gamma|_v \ge C\,e^{-d\,(N+m\,n)\,h(\alpha)}.$$

The inequalities become

$$C_1\,e^{-n\,N\,h(\alpha)} \ge |\gamma|_v \ge C_2\,e^{-d\,(N+m\,n)\,h(\alpha)}.$$

To obtain a contradiction for $d < n$ and big enough $h(\alpha)$, we need $d\,(N + m\,n) < n\,N$. If we take $N = m\,n^2$, we are done, in this case $(n-1)\,(N + m\,n) < n\,N$.

This finishes our proof of the Sprindžuk's theorem. ■

A typical Diophantine approximation proof splits into the following steps:

(1) Constructing an auxiliary function with high vanishing order at some "anchor points" (in our case it was 0).

(2) An analytic step: evaluating the auxiliary function at a point near one of the anchor points (in our case α was v-adically close to 0) and showing that this value γ is very small.

(3) Showing that the value γ is not zero. Usually it is the hardest part.

(4) Using Liouville-type inequalities to show that γ cannot be too small, contradicting (2).

26 Sprindžuk's decomposition theorem

Now we go back to theorem 20.6. Recall its statement. *Let $F(X,T) \in \mathbb{Q}[X,T]$ be a polynomial irreducible over $\mathbb{Q}$. Assume $F(0,0) = 0$ and $F'_X(0,0) \ne 0$. Let $\epsilon > 0$. For $\alpha \in \mathbb{Q}$ write down the factorization of $F(X,\alpha) \in \mathbb{Q}[X]$ into irreducible polynomials:*

$$F(X,\alpha) = f_1(X) \cdots f_r(X).$$

Then for all but finitely many $\alpha \in \mathbb{Z}$ one can write $\alpha = \alpha_1 \cdots \alpha_r$ with α_i pairwise relatively prime such that

$$\left| \frac{\log|\alpha_i|}{\log|\alpha|} - \frac{\deg f_i}{\deg_X F} \right| < \epsilon.$$

We want to generalize it for $\alpha \in \mathbb{Q}$. Of course $\log|\alpha|$ should be replaced with the height

$$h(\alpha) = h(\alpha^{-1}) = \sum_{v \in S_\alpha} \log|\alpha^{-1}|_v,$$

where $S_\alpha := \{v \in M_\mathbb{Q} \mid |\alpha|_v < 1\}$. Factorization "$\alpha = \alpha_1 \cdots \alpha_r$" does not make sense anymore if $\alpha \in \mathbb{Q}$. The right generalization is the following:

Theorem 26.1. *Let $F(X,T)$ be as above. For all but finitely many $\alpha \in \mathbb{Q}$ there exists a partition (depending on ϵ)*

$$S_\alpha = T_1 \cup \cdots \cup T_s,\ T_i \cap T_j = \emptyset \text{ for } i \neq j \quad \text{and} \quad n = d_1 + \cdots + d_s,$$

such that for each i

$$\left| \frac{\sum_{v \in T_i} \log |\alpha^{-1}|_v}{h(\alpha)} - \frac{d_i}{n} \right| < \epsilon.$$

The proof goes among the same lines. It is sufficient to show that for all but finitely many α there exists a partition such that

$$\frac{\sum_{v \in T_i} \log |\alpha^{-1}|_v}{h(\alpha)} \geq \frac{d_i}{n} - \epsilon.$$

Indeed, that is because $\sum_{1 \leq i \leq s} \frac{\sum_{v \in T_i} \log |\alpha^{-1}|_v}{h(\alpha)} = 1$ and $\sum_{1 \leq i \leq s} \frac{d_i}{n} = 1$.

For $v \in S_\alpha$ we define $v \in T_i$ if the v-adic sum β of $x(t)$ at $t = \alpha$ is a root of g_i. We have $[\mathbb{Q}(\beta) : \mathbb{Q}] = d_i$. By the same argument with auxiliary functions, we produce inequalities

$$e^{-d_i (N + C(m,n))\, h(\alpha)} \leq \prod_{v \in T_i} |\gamma|_v \leq e^{-N \sum_{v \in T_i} \log |\alpha^{-1}|_v}.$$

For details see *Yuri F. Bilu, David Masser, A Quick Proof of Sprindžuk's Decomposition Theorem*, http://dx.doi.org/10.1007/978-3-540-32439-3_2

Conclusion

During this course we used p-adic numbers to prove interesting theorems that actually do not mention p-adic numbers in the original statements: the Hasse–Minkowski theorem, the Skolem–Mahler–Lech theorem, and the Sprindžuk's theorem. These three examples are of different kind.

The Hasse–Minkowski theorem is a local–global principle that connects equations over $\mathbb{Z}$ with equations over $\mathbb{Z}_p$ for all p. We note that it is valid for the case of quadrics, and studying *obstructions* to the local–global principle in the other cases is a topic of the ongoing research.

The Skolem–Mahler–Lech theorem was proved *locally*—that is, by looking at $\mathbb{Z}_p$ for *only one* suitable p and using certain properties from p-adic analysis.

Finally, the Sprindžuk's theorem was proved using heights. It is another kind of an argument, which is somewhat *quantitative*: we claim that some statement holds for all but finitely many numbers α, and this actually comes from some bound on $h(\alpha)$.

A Proof of the Eisenstein theorem

* This will be probably merged with the main text. *

The source is essentially *J. W. S. Cassels, Local Fields (London Mathematical Society Student Texts N. 3, 1986)*, p. 28–30.

Theorem. *Let* $x(T) = \sum_{n\geq 0} a_n T^n \in K[[T]]$ *be a formal power series with coefficients in a number field* K *and suppose there is a nonzero polynomial* $F(X,T) \in K[X,T]$

$$F(X,T) := g_0(T) + g_1(T)\,X + \cdots + g_{N-1}(T)\,X^{N-1} + g_N(T)\,X^N \in K[X,T], \quad g_0(T),\ldots,g_N(T) \in K[T]$$

such that

$$F(x(T),T) = g_0(T) + g_1(T)\,x(T) + \cdots + g_{N-1}(T)\,x^{N-1}(T) + g_N(T)\,x^N(T) = 0. \tag{1}$$

Then there are algebraic integers $u, v \in O_K$, $u \neq 0$, $v \neq 0$ *such that* $u\,v^n\,a_n \in O_K$ *for all* n.

Proof. We add another formal variable Y and compute

$$F(X+Y,T) = F(X,T) + F_1(X,T)\,Y + \cdots + F_N(X,T)\,Y^N, \tag{2}$$

where $F_j(X,T) \in K[X,T]$ are some polynomials. To simplify the notation we write $F_j(X)$ for $F_j(X,T)$.

Without loss of generality we may assume that $F_1(x(T)) \neq 0$, since otherwise we could operate with $F_1(X)$ instead of $F(X)$.

Consider the power series $F_1(x(T)) \in K[[T]]$. Let m be its valuation:

$$m := v(F_1(x(T))) := \{n \mid n\text{-th coefficient of } F_1(x(T)) \text{ is } \neq 0\}.$$

Now we separate $x(T)$ in two parts: the lower terms $u(T) \in K[T]$ of degree $\leq m+1$ and the "tail" $v(T) \in K[[T]]$:

$$x(T) = (\underbrace{a_0 + \cdots + a_m\,T^m + a_{m+1}\,T^{m+1}}_{=:u(T)}) + T^{m+1}\,(\underbrace{a_{m+2}\,T + a_{m+3}\,T^2 + \cdots}_{=:v(T)}) \tag{3}$$

It is enough to show that the tail $v(T)$ satisfies the claimed property for coefficients.

By (1), (2), (3) we have

$$0 = F(x(T)) = F(u(T) + T^{m+1}\,v(T)) = F(u(T)) + T^{m+1}\,F_1(u(T))\cdot v(T) + \sum_{j\geq 2} T^{(m+1)\,j}\,F_j(u(T))\cdot v(T)^j,$$

where $F(u(T)), F_1(u(T)), F_j(u(T)) \in K[T]$ are certain polynomials. All the summands except for perhaps the first are divisible by T^{2m+1} by our choice of m, and so $F(u(T))$ should be divisible by T^{2m+1} as well (in $K[T]$). Dividing the identity by T^{2m+1}, we obtain

$$0 = f(T) + f_1(T)\,v(T) + f_2(T)\,v(T)^2 + \cdots + f_N(T)\,v(T)^N, \tag{4}$$

where $f(T), f_1(T),\ldots,f_N(T) \in K[T]$ are some polynomials, and by our choice of m their free terms are

$$\ell := f_1(0) \neq 0 \text{ and } f_j(0) = 0 \text{ for } j > 1.$$

After multiplying (4) by certain algebraic integer, we may assume that $f, f_1, \ldots, f_N \in O_K[T]$.

Observe that by its construction, in the power series $v(T) = \sum_{n\geq 1} b_n\,T^n$ (where $b_n = a_{n+m+1}$) the constant term is 0. We want to show that $\ell^n\,b_n \in O_K$.

We look at the coefficients of T^n in (4):

$$0 = f(T) + f_1(T)\cdot\left(\sum_{n\geq 1} b_n\, T^n\right) + f_2(T)\cdot\left(\sum_{n\geq 1}\left(\sum_{n_1+n_2=n} b_{n_1}\, b_{n_2}\right) T^n\right) + \cdots +$$
$$f_N(T)\cdot\left(\sum_{n\geq 1}\left(\sum_{n_1+\cdots+n_N=n} b_{n_1}\cdots b_{n_N}\right) T^n\right).$$

Using the fact that the free term of $f_1(T)$ is ℓ and it is 0 for $f_2(T),\ldots,f_N(T)$, we can express $\ell\, b_n$ as the sum of terms of the type $c\prod_{i<n} b_i^{k_i}$, where $c\in O_K$. Now $\ell^n\, b_n\in O_K$ follows by induction.