CIMPA school: Arithmetic, coding and cryptography

Written by Margherita Pagano

April 12, 2026

These are the lecture notes of the second part of the course of *Arithmetic Number Theory* at the CIMPA school on Arithmetic, coding and cryptography at the National Higher School of Mathematics Sidi Abdellah (Algiers), Algeria.

Beware of typos/mistakes. Corrections are welcome, you can write me at m.pagano@imperial.ac.uk.

1 Lecture 1 (9/04/2026)

1.1 Motivation

Let $K/\mathbf{Q}$ be a number field. In order to understand the arithmetic of K, we would like to know for every prime p the splitting behaviour of the ideal $p \cdot \mathcal{O}_K$. At this point, the strongest tool we have is the Kummer-Dedekind's criteria.

Theorem 1.1 (Kummer-Dedekind)**.** *Let $\alpha \in \mathcal{O}_K$ be such that $\mathbf{Q}(\alpha) = K$. If $p \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$ then we can read the splitting behaviour of p in $\mathcal{O}_K$ from the reduction of $\min_\alpha(x) \in \mathbf{Z}[x]$ modulo p. More precisely, if $\min_\alpha(x)$ factors over $\mathbf{F}_p[x]$ as*

$$\overline{\min}_\alpha(x) = \prod_{i=1}^{t} \bar{g}_i^{e_i}(x)$$

with $\bar{g}_i$ distinct irreducible polynomials, then

$$p \cdot \mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdot \dots \cdot p_t^{e_t}$$

with $\mathfrak{p}_i = (p, g_i(\alpha))$ with $g_i(x) \in \mathbf{Z}[x]$ any lift of $\bar{g}_i(x)$.

Remark 1.2. It can happen that there exists a prime p such that for all $\alpha \in \mathcal{O}_K$ for which $K = \mathbf{Q}(\alpha)$ we have $p \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$ (cf. Example 2.7).

Question: what to do in this case?

Aim of the second part of course: to get around this issue.

We will show that for every prime p we can build a field extension $\mathbf{Q}_p$ of $\mathbf{Q}$, that can be used to determine $p \cdot \mathcal{O}_K$. More precisely, we will see that if

$$p \cdot \mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdot \dots \cdot \mathfrak{p}_t^{e_t}$$

then

$$K \otimes_{\mathbf{Q}} \mathbf{Q}_p \simeq \prod_{i=1}^{t} K_{\mathfrak{p}_i}$$

with $K_{\mathfrak{p}_i}/\mathbf{Q}_p$ finite such that $[K_{\mathfrak{p}_i} : \mathbf{Q}_p] = e_i \cdot f_i$.

Remark 1.3. If $K = \mathbf{Q}(\alpha) = \frac{\mathbf{Q}[x]}{(f(x))}$, then

$$K \otimes_{\mathbf{Q}} \mathbf{Q}_p = \frac{\mathbf{Q}[x]}{(f(x))} \otimes_{\mathbf{Q}} \mathbf{Q}_p \simeq \frac{\mathbf{Q}_p[x]}{(f(x))}$$

hence in order to understand the $K_{\mathfrak{p}_i}$ we will need to understand the factorisation of $f(x)$ in $\mathbf{Q}_p[x]$ into irreducible factors. Indeed, if

$$f(x) = h_1(x) \dots h_t(x)$$

with $h_i(x) \in \mathbf{Q}_p[x]$ irreducible, then by the Chinese reminder theorem

$$\frac{\mathbf{Q}_p[x]}{(f(x))} \simeq \prod_{i=1}^{t} \frac{\mathbf{Q}_p[x]}{(h_i(x))}$$

and $K_{\mathfrak{p}_i} \leftrightarrow \frac{\mathbf{Q}_p[x]}{(h_i(x))}$.

By a matter of contrast, if instead of $\mathbf{Q}_p$ we take $\mathbf{R}$, we have

$$K \otimes_{\mathbf{Q}} \mathbf{R} \simeq \frac{\mathbf{R}[x]}{(f(x))}$$

and we know that

$$f(x) = (x - \alpha_1) \dots (x - \alpha_r) \cdot h_1(x) \dots h_s(x)$$

with $h_i(x)$ irreducible of degree 2, and $n = r + 2s$. In particular,

$$K \otimes_{\mathbf{Q}} \mathbf{R} \simeq \prod_{i=1}^{r} \frac{\mathbf{R}[x]}{(x - \alpha_i)} \times \prod_{j=1}^{s} \frac{\mathbf{R}[x]}{(h_j(x))} \simeq \mathbf{R}^r \times \mathbf{C}^s$$

and r is the number of real embeddings of the number field, while s is the number of pairs of conjugate complex embeddings.

1.2 Real numbers

We start by revisiting how, using the Euclidean metric, it is possible to build the real numbers as a completion of the rational numbers. We will point out which are the key property we are using to perform this construction. We will later see how, in analogy with $\mathbf{R}$, also the field of p-adic numbers $\mathbf{Q}_p$ is defined as the completion of $\mathbf{Q}$ with respect to some metric, namely the *p-adic absolute value*.

On the rational numbers we have the Euclidean absolute value

$$\begin{aligned} \phi_\infty \colon \mathbf{Q} &\to \mathbf{Q}_{\geq 0} \\ x &\mapsto |x|. \end{aligned}$$

This absolute value induces a topology on $\mathbf{Q}$ in which a basis of open neighborhoods of a point $x \in \mathbf{Q}$ is given by

$$U(x, \epsilon) = \{y \in K \mid |x - y| < \epsilon\} = (x - \epsilon, x + \epsilon) \cap \mathbf{Q}.$$

The real numbers are the completion of the rational numbers with respect to the euclidean metric. A possible way to construct them is by using the notion of Cauchy sequences.

Definition 1.4. Let $(a_n)_{n\in\mathbf{N}}$ be a sequence of elements of $\mathbf{Q}$. Then, $(a_n)_{n\in\mathbf{N}}$ is a Cauchy sequence if for every $\epsilon > 0$ there exists $N > 0$ such that for all $m, n \geq N$ we have

$$\phi_\infty(a_n - a_m) = |a_n - a_m| < \epsilon.$$

We define

$$\mathfrak{R} := \{(a_n)_{n\in\mathbf{N}} \mid a_n \in \mathbf{Q}, \text{ is a Cauchy sequence}\}.$$

We say that a Cauchy sequence *tends to* 0 if for all $\epsilon > 0$ there exists $N > 0$ such that for all $n \geq N$, $\phi_\infty(a_n) < \epsilon$. We define

$$\mathfrak{m} := \{(a_n)_{n\in\mathbf{N}} \in \mathfrak{R} \mid (a_n)_{n\in\mathbf{N}} \text{ tends to } 0\}.$$

It is possible to show that (cf. Exercise 3.1).

- $\mathfrak{R}$ with component-wise sum and multiplication is a ring.
- $\mathfrak{R}/\mathfrak{m}$ is a field (for this we need to check that if $(a_n)_{n\in\mathbf{N}}$ is a Cauchy sequence that does not tend to zero, then there exists $(b_n)_{n\in\mathbf{N}} \in \mathfrak{R}$ such that $(a_n \cdot b_n - 1) \in \mathfrak{m}$).

In particular, this implies that the quotient $\mathfrak{R}/\mathfrak{m}$ is a **field**. We can define $\mathbf{R}$ as

$$\mathfrak{R}/\mathfrak{m}.$$

1.3 p-adic valuation on rational numbers

Every element $x \in \mathbf{Q}$ can be written in a unique way as $x = \frac{a}{b}$ with $a, b \in \mathbf{Z}$, $b \neq 0$ and $\gcd(a, b) = 1$.

Let p be a prime number. We define

$$\mathbf{Z}_{(p)} := \left\{\frac{a}{b} \in \mathbf{Q} \mid p \nmid b\right\} \subseteq \mathbf{Q}$$

Lemma 1.5. *We have the following properties.*

1. $\mathbf{Z}_{(p)}$ *is a ring;*
2. *it is local with maximal ideal given by* $p\mathbf{Z}_{(p)}$ *and residue field* $\mathbf{F}_p$*;*
3. *its fraction field is* $\mathbf{Q}$*.*

Proof. Point 1. follows from a way more general construction. It is the localisation $\mathbf{Z}_{(p)} = S^{-1}\mathbf{Z}$ of $\mathbf{Z}$ with respect to the multiplicative system $S = \mathbf{Z} \setminus (p)$. Also point 2 belongs to a more general construction and the fact that $\mathbf{Z}/p\mathbf{Z} \simeq \mathbf{F}_p$. For point three, note that since $\mathbf{Z}_{(p)} \subseteq \mathbf{Q}$, we have $\mathrm{Frac}(\mathbf{Z}_{(p)}) \subseteq \mathbf{Q}$, on the other hand if we denote by $\mathbf{Z}_{(p)}[1/p]$ the smallest subring of $\mathbf{Q}$ containing both $\mathbf{Z}_p$ and $1/p$, then

$$\mathbf{Z}_{(p)}\left[\frac{1}{p}\right] = \mathbf{Q} \subseteq \mathrm{Frac}(\mathbf{Z}_{(p)}) \subseteq \mathbf{Q}.$$

□

We define

$$\begin{aligned} \mathrm{ord}_p \colon \mathbf{Z}_{(p)} \setminus \{0\} &\to \mathbf{N} \\ \frac{a}{b} &\mapsto \mathrm{ord}_p(a). \end{aligned}$$

We extend this map to 0 by putting $\mathrm{ord}_p(0) = \infty$. In particular,

$$\{x \in \mathbf{Z}_{(p)} \mid \mathrm{ord}_p(x) \geq 1\} = p\mathbf{Z}_{(p)}.$$

We can now extend the map ord_p as a map from $\mathbf{Q}$ to $\mathbf{Z}$, by setting

$$\mathrm{ord}_p(x/y) := \mathrm{ord}_p(x) - \mathrm{ord}_p(y).$$

One can check

1. $\mathrm{ord}_p(x \cdot y) = \mathrm{ord}_p(x) + \mathrm{ord}_p(y)$;
2. $\mathrm{ord}_p(x + y) \geq \min\{\mathrm{ord}_p(x), \mathrm{ord}_p(y)\}$ with equality if $\mathrm{ord}_p(x) \neq \mathrm{ord}_p(y)$.

Example 1.6. Let $p = 5$. Then

- $\mathrm{ord}_5(7) = 0$.
- $\mathrm{ord}_5(100) = \mathrm{ord}_5(5^2 \cdot 4) = \mathrm{ord}_5(5^2) + \mathrm{ord}_5(4) = 2$.
- $\mathrm{ord}_5(4/125) = \mathrm{ord}_5(4) - \mathrm{ord}_5(5^3) = -3$.

Let $c \in (0, 1)$ be a real number, then we define the p-adic absolute value as

$$\begin{aligned} \phi_p \colon \mathbf{Q} &\to \mathbf{R}_{\geq 0} \\ x &\mapsto c^{\mathrm{ord}_p(x)} \end{aligned}$$

Example 1.7. Let $p = 5$. Then

- $\mathrm{ord}_5(7) = 1$, hence $\phi_5(7) = c^0 = 1$
- $\mathrm{ord}_5(25) = 2$, hence $\phi_5(25) = c^2$.
- $\mathrm{ord}_5(3/125) = \mathrm{ord}_5(3) - \mathrm{ord}_5(5^3) = -3$, hence $\phi_5(3/125) = c^{-3}$.

Note that, since $c < 1$ we have $\phi_5(\alpha/\beta)$ with $\gcd(\alpha, \beta) = 1$ is small when α is divisible by a high power of 5 and it is big when β is divisible by a high power of 5.

Exercise 1.8. Show that for any $x \in \mathbf{Q}$ we have $\phi_p(x) = 1$ for all but finitely many primes.

It has the following properties

1. $\phi_p(x) = 0$ if and only if $x = 0$;
2. $\phi_p(xy) = \phi_p(x)\phi_p(y)$;
3. $\phi_p(x + y) \leq \max\{\phi_p(x), \phi_p(y)\}$ (with equality if $\phi_p(x) \neq \phi_p(y)$).

In this case, the induced topology will have a basis of open neighbourhoods of a point $x \in \mathbf{Q}$ given by

$$U(x, \epsilon) = \{y \in \mathbf{Q} \mid \phi_p(x - y) < \epsilon\}$$

Remark 1.9. Let's look at $x = 0$, then $y = p^r \cdot \frac{a}{b}$ and

$$\phi_p(y) = c^{\mathrm{ord}_p(y)} < \epsilon \Leftrightarrow \mathrm{ord}_p(y) > \log_c \epsilon \Leftrightarrow r > \log_c \epsilon.$$

Namely, elements close to 0 are those highly divisible by p.

Definition 1.10. $\mathbf{Q}_p$ is defined as the completion of $\mathbf{Q}$ with respect to the p-adic absolute value ϕ_p. In particular, in analogy with $\mathbf{R}$, we define

$$\mathfrak{R} := \{\text{Cauchy sequences with respect to } \phi_p\}$$

with componentwise addition and multiplication. I.e. $(a_n)_{n\in\mathbf{N}}$ lies in $\mathfrak{R}$ if and only if $\forall \epsilon > 0$ there exists $M_\epsilon > 0$ such that for all $n, m > M_\epsilon$

$$\phi_p(x_n - x_m) \leq \epsilon.$$

We define

$$\mathfrak{m} := \{(a_n)_{n\in\mathbf{N}} \in \mathfrak{R} \mid (a_n)_{n\in\mathbf{N}} \text{ tends to } 0\}.$$

In analogy with $\mathbf{R}$, one can check that the quotient $\mathfrak{R}/\mathfrak{m}$ is a field, cf. Exercise 3.3.

Remark 1.11. Note that if $(x_n)_{n\in\mathbf{N}}$ is a Cauchy sequence, then also $(\phi_p(x_n))_{n\in\mathbf{N}}$ is a Cauchy sequence of elements in $\mathbf{R}_{\geq 0}$. Hence, it admit a limit ($\mathbf{R}$ is complete!). Using this remark, we see that the valuation ϕ_p extend to $\mathbf{Q}_p$, by setting

$$\phi_p(x) = \phi_p((x_n)) = \lim_{n\to\infty} \phi_p(x_n).$$

2 Lecture 2 (12/04/2026)

2.1 Arithmetic aspects of $\mathbf{Q}_p$

We define $\mathbf{Z}_p \subseteq \mathbf{Q}_p$ as

$$\mathbf{Z}_p := \{x \in \mathbf{Q}_p \mid \phi_p(x) \leq 1\} = \{x \in \mathbf{Q}_p \mid \mathrm{ord}_p(x) \geq 0\}.$$

Remark 2.1. $\mathbf{Z}_p$ is a ring, in fact, if $\phi_p(x), \phi_p(y) \leq 1$, then

$$\phi_p(x + y) \leq \max\{\phi_p(x), \phi_p(y)\} \leq 1$$

and

$$\phi_p(xy) = \phi_p(x) \cdot \phi_p(y) \leq 1.$$

Moreover, let I be a non-zero prime ideal in $\mathbf{Z}_p$, then

$$I = p\mathbf{Z}_p = \{x \in \mathbf{Z}_p \mid \phi_p(x) > 0\} = \{x \in \mathbf{Z}_p \mid \mathrm{ord}_p(x) \geq 1\}.$$

In fact, if $I \subseteq \mathbf{Z}_p$, then we can take $x \in I$ with minimal valuation, then $\mathrm{ord}_p(x) \geq 1$ (since elements with order 0 are invertible in $\mathbf{Z}_p$). Moreover,

$$\mathrm{ord}_p(xp^{-\mathrm{ord}_p(x)}) = 0 \Rightarrow p^r = u \cdot x, \text{ with } u \in \mathbf{Z}_p^\times$$

hence $p^r \in I$, which if I is prime implies that $p \in I$, namely $p\mathbf{Z}_p \subseteq I$. On the other hand, cf. Exercise 3.4

$$\frac{\mathbf{Z}_p}{p\mathbf{Z}_p} \simeq \mathbf{F}_p.$$

2.2 Representing elements in $\mathbf{Q}_p$

Theorem 2.2. *Every element $x \in \mathbf{Q}_p$ can be written uniquely as a convergent series*

$$\sum_{n=k}^{\infty} a_n p^n, \quad \text{with } a_n \in \{0, \dots, p-1\},\ k \in \mathbf{Z}.$$

Proof. Let $(a_n)_{n \geq k}$ with $k \in \mathbf{Z}$ and $a_i \in \{0, \dots, p-1\}$ be any sequence, then the sum

$$\sum_{n=k}^{\infty} a_n p^n$$

converges. By construction of $\mathbf{Q}_p$ it is enough to show that the sequence

$$S_N := \sum_{n=k}^{N} a_n p^n$$

is Cauchy. Note that for $M > N$

$$\phi_p(S_M - S_N) = \phi_p(\sum_{n=N+1}^{M} a_n p^n) \leq \max_{n=N+1,\dots,M} \{c^{\mathrm{ord}_p(a_n p^n)}\} = c^{N+1} \xrightarrow{N \to \infty} 0,$$

hence we are done.

Take $x \in \mathbf{Q}_p$, then $p^n x \in \mathbf{Z}_p$ for some n. In fact, if $\phi_p(x) > 1$, then take n such that $\phi_p(x) < c^{-n}$ (this always exists since $c < 1$ and hence $c^{-n} \xrightarrow{n \to \infty} \infty$), then $\phi_p(p^n x) = c^n \cdot \phi_p(x) \leq 1$.

It is therefore enough to show that every element in $\mathbf{Z}_p$ can be written as $\sum_{n=0}^{\infty} a_n p^n$ with $a_n \in \{0, \dots, p-1\}$. We are going to use that $\mathbf{Z}_p / p\mathbf{Z}_p \simeq \mathbf{F}_p$.

In particular, let a_0 be the unique element in $\{0, \dots, p-1\}$ such that $x \equiv a_0 \mod p$, then $x = a_0 + p \cdot x_1$ for some $x_1 \in \mathbf{Z}_p$. Iterating the procedure we get the expression we want. □

We have also proven the following corollary.

Corollary 2.3. *Any element in $\mathbf{Z}_p$ can be written as*

$$\sum_{k=0}^{\infty} a_n p^n$$

for some $a_n \in \{0, \dots, p-1\}$. In particular, for any $n \geq 1$ we have

$$\mathbf{Z}_p / p^n \mathbf{Z}_p \simeq \mathbf{Z} / p^n \mathbf{Z}.$$

2.3 Hensel's lemma

We start with the following observation: let $f(x) \in \mathbf{Z}[x]$ be a polynomial. If over $\mathbf{Q}_p$ there exists $\alpha \in \mathbf{Q}_p$ such that $f(\alpha) = 0$, then

$$f(x) = (x - \alpha) \cdot f_1(x).$$

(this is true over every polynomial ring $K[x]$ with K field, it follows from the existence of division with reminder on $K[x]$).

We start with a first version of Hensel's lemma, which allows us to lift solution of polynomial equations modulo p to solutions in $\mathbf{Z}_p$.

The idea behind it is relatively simple: let $f(T) \in \mathbf{Z}[T]$ be a polynomial and assume that there exists a prime p such that

$$\bar{f}(T) = 0 \text{ has a solution over } \mathbf{Z}/p\mathbf{Z} = \mathbb{F}_p.$$

Let $\bar{\alpha}_1 \in \mathbf{Z}/p\mathbf{Z}$ be such an element, and $\alpha_1 \in \mathbf{Z}$ be such that

$$\alpha_1 \equiv \bar{\alpha}_1 \mod p.$$

Assume now that we can continue the procedure by finding $\alpha_2 \in \mathbf{Z}$ such that

$$\overline{f(\alpha_2)} \equiv 0 \mod p^2$$

and

$$\overline{\alpha_2} \equiv \overline{\alpha_1} \mod p$$

and so on and so forth. In this case we would have a sequence $(\alpha_n)_{n\in\mathbf{N}}$ of elements of $\mathbf{Z}$ such that for $m > n$,

$$\mathrm{ord}_p(\alpha_m - \alpha_n) \geq p^n \Rightarrow \phi_p(\alpha_m - \alpha_n) \leq c^{p^n} \xrightarrow{n\to\infty} 0.$$

In particular, it is a Cauchy sequence and therefore in $\mathbf{Z}_p$ it will converge to an element α such that

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

$$\mathrm{ord}_p(f(\alpha_n)) \geq p^n \Rightarrow \phi_p(f(\alpha_n)) \xrightarrow{n\to\infty} 0.$$

At this point, we would like to have some conditions that allows to be sure that such a sequence exists.

Lemma 2.4 (Hensel's lemma)**.** *Let $f \in \mathbf{Z}_p[T]$ be a polynomial. Let $x_0 \in \mathbf{Z}_p$ be an element for which*

$$\phi_p(f(x_0)) < \phi_p(f'(x_0))^2$$

then there exists $x \in \mathbf{Z}_p$ such that $f(x) = 0$ and

$$\phi_p(x - x_0) \leq \phi_p(f(x_0)/f'(x_0)).$$

Remark 2.5. Recall that $x_0 = \sum_{n=0}^{\infty} a_n p^n$. In particular, if $a_0 \in \{0, \ldots, p-1\}$ is such that

$$\bar{f}(a_0) = 0, \text{ in } \mathbf{F}_p$$

and

$$\bar{f}'(a_0) \neq 0, \text{ in } \mathbf{F}_p$$

then $\phi_p(f(x_0)) = c^{\mathrm{ord}_p(f(x_0))} < 1$ and $\phi_p(f'(x_0)) = c^{\mathrm{ord}_p(f'(x_0))} = 1$. Hence, by Hensel's lemma there is an element $x \in \mathbf{Z}_p$ such that $f(x) = 0$ and $\phi_p(x - x_0) = c^{\mathrm{ord}_p(x-x_0)} < 1$, namely $x \equiv x_0 \mod p$.

Proof of Hensel's lemma. The proof is essentially Newton's method. Let us start by defining

$$m_0 := \mathrm{ord}_p(f(x_0)), \quad \text{and} \quad n_0 := \mathrm{ord}_p(f'(x_0)).$$

By assumption $x_0 \in \mathbf{Z}_p$ is such that

$$m_0 = \mathrm{ord}_p(f(x_0)) \geq \mathrm{ord}_p(f'(x_0)^2) + 1 =: 2n_0 + 1.$$

In particular,

$$f(x_0) \equiv 0 \mod p^{2n_0+1}.$$

We define

$$x_1 := x_0 - \frac{f(x_0)}{f'(x_0)}.$$

Fact: if $g \in \mathbf{Z}_p[x]$ is a polynomial, then for every $x, y \in \mathbf{Z}_p$ there exists $z \in \mathbf{Z}_p$ such that

$$g(x+y) = g(x) + g'(x)y + zy^2.$$

In particular,

$$f(x_1) = f\left(x_0 - \frac{f(x_0)}{f'(x_0)}\right) = f(x_0) - f'(x_0)\frac{f(x_0)}{f'(x_0)} + z \cdot \left(\frac{f(x_0)}{f'(x_0)}\right)^2 = z \cdot \left(\frac{f(x_0)}{f'(x_0)}\right)^2$$

and

$$m_1 := \mathrm{ord}_p(f(x_1)) \geq \mathrm{ord}_p\left(\left(\frac{f(x_0)}{f'(x_0)}\right)^2\right) \geq 4n_0 + 2 - 2n_0 = 2n_0 + 2.$$

Hence

$$f(x_1) \equiv 0 \mod p^{2n_0+2}.$$

Moreover, if we apply the fact above again, we can write

$$f'(x_1) = f'(x_0) + \frac{f(x_0)}{f'(x_0)} \cdot z_1$$

and get that

$$n_1 := \mathrm{ord}_p(f'(x_1)) = \mathrm{ord}_p\left(f'(x_0) + \frac{f(x_0)}{f'(x_0)}z_1\right) = \mathrm{ord}_p(f'(x_0)).$$

The last equality follows from the fact that

$$\mathrm{ord}_p\left(\frac{f(x_0)}{f'(x_0)}z_1\right) \geq \mathrm{ord}_p\left(\frac{f(x_0)}{f'(x_0)}\right) > \mathrm{ord}_p(f'(x_0)).$$

Therefore, the sequence

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}.$$

is well defined and will converge since

$$\phi_p(x_{n+1} - x_n) = \phi_p(f(x_n)/f'(x_n)) \geq 2n_0 + 1 + n - n_0 = n_0 + 1 + n \xrightarrow{n\to\infty} \infty.$$

□

Example 2.6. Let $K = \mathbf{Q}(\sqrt{-13}) = \mathbf{Q}[x]/(x^2+13)$. Let $f(x) := x^2+13$, then for $p = 7$, we see that

$$f(1) = 14 \equiv 0 \mod 7$$

and $f'(x) = 2x$ is such that

$$f'(1) = 2 \not\equiv 0 \mod 7.$$

In particular,

$$\mathrm{ord}_7(f(1)) = \mathrm{ord}_7(14) = 1, \Rightarrow \phi_7(f(1)) = c$$

and

$$\mathrm{ord}_7(f'(1)) = 0, \Rightarrow \phi_7(f'(1)) = c^0 = 1.$$

In particular,

$$\phi_p(f(1)) < \phi_p(f'(1))^2$$

and hence by Hensel's lemma there exists $\alpha \in \mathbf{Z}_7$ such that $f(\alpha) = 0$ and $\alpha \equiv 1 \mod 7$. We therefore have

$$f(\alpha) = (x-\alpha)(x-\beta), \text{ in } \mathbf{Q}_7[x].$$

In particular,

$$\mathbf{Q}(\sqrt{-13}) \otimes_{\mathbf{Q}} \mathbf{Q}_7 \simeq \mathbf{Q}_7 \times \mathbf{Q}_7.$$

Exercise: compare it with what Kummer-Dedekind's criteria gives.

Example 2.7. Let $f(x) = x^3 - x^2 - 2x - 8$. Then,

$$f'(x) = 3 \cdot x^2 - 2 \cdot x - 2$$

If we work modulo 16, then we have

$$f(7) = 272 \equiv 0 \mod 16, \Rightarrow \mathrm{ord}_2(f(7)) \geq 4 \Rightarrow \phi_2(f(7)) \leq c^4$$

and

$$f'(7) = 131 \Rightarrow \mathrm{ord}_2(f'(7)) = 0 \Rightarrow \phi_2(f'(7)) = 0.$$

Moreover,

$$f(6) = 160 \equiv 0 \mod 16, \Rightarrow \mathrm{ord}_2(f(6)) \geq 4 \Rightarrow \phi_2(f(6)) \leq c^4$$

and

$$f'(6) = 94 = 2 \cdot 47, \Rightarrow \mathrm{ord}_2(f'(6)) = 1 \Rightarrow \phi_2(f'(6)) = c$$

and

$$f(12) = 1552 \equiv 0 \mod 16, \Rightarrow \mathrm{ord}_2(f(12)) \geq 4 \Rightarrow \phi_2(f(12)) \leq c^4$$

while

$$f'(12) = 406 = 2 \cdot 203, \Rightarrow \mathrm{ord}_2(f'(6)) = 1 \Rightarrow \phi_2(f'(12)) = c.$$

In all these cases we can apply Hensel's lemma and get three different roots, $\alpha_1, \alpha_2, \alpha_3$ in $\mathbf{Z}_2$ such that

$$\mathrm{ord}_2(\alpha_1 - 7) \leq c^4, \Rightarrow \alpha_1 \equiv 7 \mod 2^4 = 16$$

and

$$\mathrm{ord}_2(\alpha_2 - 6) \leq c^3, \Rightarrow \alpha_2 \equiv 6 \mod 2^3 = 8$$

and

$$\mathrm{ord}_2(\alpha_3 - 12) \leq c^3, \Rightarrow \alpha_3 \equiv 4 \mod 2^3 = 8.$$

In particular,

$$K \otimes_{\mathbf{Q}} \mathbf{Q}_2 = \frac{\mathbf{Q}_2[x]}{(x^3 - x^2 - x - 8)} \simeq \frac{\mathbf{Q}_2[x]}{(x - \alpha_1)} \times \frac{\mathbf{Q}_2[x]}{(x - \alpha_2)} \times \frac{\mathbf{Q}_2[x]}{(x - \alpha_3)} \simeq \mathbf{Q}_2 \times \mathbf{Q}_2 \times \mathbf{Q}_2.$$

If we use (even if we did not prove it so far) that there exists a correspondence between the factorisation of $f(x)$ in $\mathbf{Q}_p$ and the one of the prime p in $K = \mathbf{Q}[x]/(f(x))$ where α is a root of f, then we get that there must be three *different* primes above 2, namely (for degree reason)

$$2 \cdot \mathcal{O}_K = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3.$$

Finally, note that we could have never get this result from Kummer-Dedekind's criteria. In fact, assume that there exists $\theta \in K$ such that $2 \nmid [\mathcal{O}_K : \mathbf{Z}[\theta]]$, then the factorisation of 2 can be read from the reduction modulo 2 of the minimal polynomial of θ, which will be an irreducible polynomial of degree 3. However, polynomials of degree 3 in $\mathbf{F}_2$ cannot decompose as three *different* linear factors.

3 Theoretical exercises

This is a list of exercises aimed to fill in the gaps of the omitted details during the lectures.

Exercise 3.1. The aim of this exercise is to give a full proof of the construction of real numbers, cf. Section 1.2.

1. Show that if $(a_n)_{n\in\mathbf{N}}$ and $(b_n)_{n\in\mathbf{N}}$ are elements of $\mathfrak{R}$, then

   (a) $(a_n + b_n)_{\mathfrak{n}\in\mathbf{N}} \in \mathfrak{R}$;

   (b) $(a_n \cdot b_n)_{n\in\mathbf{N}} \in \mathfrak{R}$.

   Deduce that $\mathfrak{R}$ with component-wise addition and multiplication is a ring.

2. Show that if $(a_n)_{n\in\mathbf{N}}$ and $(b_n)_{n\in\mathbf{N}}$ are elements of $\mathfrak{m}$, then

   $$(a_n + b_n)_{n\in\mathbf{N}} \in \mathfrak{m}.$$

   Show that if $(a_n)_{n\in\mathbf{N}} \in \mathfrak{m}$ and $(c_n)_{n\in\mathbf{N}} \in \mathfrak{R}$, then

   $$(c_n \cdot a_n)_{n\in\mathbf{N}} \in \mathfrak{m}.$$

   Deduce that $\mathfrak{m}$ is an ideal of $\mathfrak{R}$.

   [Hint: show that if $(b_n)_{n\in\mathbf{N}}$ is a Cauchy sequence that does not tend to zero, then there exists N such that for all $n \geq N$, $b_n \neq 0$].

3. Show that if $(b_n)_{n\in\mathbf{N}}$ is a Cauchy sequence that does not tend to zero, then there exists a Cauchy sequence $(c_n)_{n\in\mathbf{N}}$ such that

   $$(b_n \cdot c_n - 1)_{n\in\mathbf{N}} \in \mathfrak{m}.$$

   Deduce that $\mathfrak{m}$ is a maximal ideal of $\mathfrak{R}$.

4. Using that $\mathbf{Q}$ is dense in $\mathbf{R}$ with respect to the euclidean metric, show that

   $$\mathfrak{R}/\mathfrak{m} \simeq \mathbf{R}.$$

Exercise 3.2. Prove the following properties

1. $\mathrm{ord}_p(xy) = \mathrm{ord}_p(x) + \mathrm{ord}_p(y)$;
2. $\mathrm{ord}_p(x+y) \geq \max\{\mathrm{ord}_p(x), \mathrm{ord}_p(y)\}$ with equality if $\mathrm{ord}_p(x) \neq \mathrm{ord}_p(y)$.

Exercise 3.3. Check that in Exercise 3.1 all the steps holds true if we replace ϕ_∞ with ϕ_p.

Exercise 3.4. Show that

$$\frac{\mathbf{Z}_p}{p\mathbf{Z}_p} \simeq \mathbf{F}_p$$

[Hint: use that $\mathbf{Z}$ is dense in $\mathbf{Z}_p$].

Exercise 3.5. Show that the metric space $\mathbf{Q}_p$ (with distance function given by $d(x,y) = \phi_p(x-y)$) has the following properties.

1. Every triangle in $\mathbf{Q}_p$ is isosceles, i.e. given three points $x, y, z \in \mathbf{Q}_p$ there is one that has equal distances to the two others;
2. Every point x in the open ball $U(x_0, \epsilon)$ of radius ϵ around $x_0 \in \mathbf{Q}_p$ is a center, i.e. $U(x, \epsilon) = U(x_0, \epsilon)$. Here

$$U(x_0, \epsilon) := \{x \in \mathbf{Q}_p \mid \phi_p(x - x_0) < \epsilon\}.$$