Exercises (v21/09/03) (Carls/Edixhoven)

EX.1: CONSTRUCTION OF THE p-ADIC NUMBERS

Let p be a prime number. Every non-zero rational number z has a unique representation

$$z = p^i \frac{a}{b},$$

where $\gcd(ab, p) = 1$ and $i \in \mathbb{Z}$. We set $v(z) := i$. This defines a group homomorphism $v : \mathbb{Q}^* \to \mathbb{Z}$. Further we set

$$|z|_p := p^{-v(z)} \quad \text{and} \quad |0|_p := 0.$$

This defines an absolute value on $\mathbb{Q}$, the *p-adic absolute value*. Together with this absolute value the set $\mathbb{Q}$ is a metric space and we can form the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$. The completion is given by the set of all Cauchy sequences in $\mathbb{Q}$, where we consider two sequences as equivalent if they differ by a sequence converging to zero. The completion is denoted by $\mathbb{Q}_p$. Its elements are called *p-adic numbers*. The set $\mathbb{Q}_p$ inherits the operations of addition and multiplication from the field $\mathbb{Q}$.

(a) Show that $\mathbb{Q}_p$ is a field.

The natural map $\mathbb{Q} \to \mathbb{Q}_p$ mapping a rational number to the corresponding constant sequence is injective. Hence we can consider $\mathbb{Q}$ as subfield of $\mathbb{Q}_p$. The absolute value $|\cdot|_p$ extends to $\mathbb{Q}_p$ by setting

$$\Big|\ [(x_0, x_1, \ldots)]\ \Big|_p := \lim_{k\to\infty} |x_k|_p.$$

Here the brackets indicate that we are working with equivalence classes.

(b) Prove that $\mathbb{Q}_p$ is complete with respect to the absolute value $|\cdot|_p$ and that $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. (You might prove this in greater generality for the completion of an arbitrary metric space.)

In the lecture notes the p-adic numbers are introduced as Laurent series in p. We want to show that the two definitions coincide. First of all note that a series with terms in $\mathbb{Q}_p$ converges if and only if its terms tend to zero. This follows from

$$|z + y|_p \leq \max\{|z|_p, |y|_p\}, \tag{1}$$

which is called the *ultrametric inequality*. If $|z|_p \neq |y|_p$, then equality holds.
The elements of the set

$$\mathbb{Z}_p := \{\ x \in \mathbb{Q}_p \ \mid\ |x|_p \leq 1\ \}$$

are called *p-adic integers*. They form a ring, because of (1) and $|z \cdot y|_p = |z|_p \cdot |y|_p$. Note that every p-adic integer can be represented by a Cauchy sequence of integers. Hence $\mathbb{Z}_p$ equals the completion of the metric space $\mathbb{Z}$ with respect to the absolute value $|\cdot|_p$.

(c) Show that every non-zero p-adic integer $z \in xz_p$ has a unique representation

$$z = \sum_{i=0}^{\infty} z_i p^i,$$

where $0 \le z_i < p$ and $|z|_p = p^{-j}$, where $j := \min\{\ i \ge 0 \ |\ z_i \ne 0\ \}$.

We should mention that there is also an algebraic way of constructing the p-adic integers. One takes the limit of the inverse system

$$\mathbb{Z}/p\mathbb{Z} \leftarrow \mathbb{Z}/p^2\mathbb{Z} \leftarrow \mathbb{Z}/p^3\mathbb{Z} \dots.$$

If we replace p by an arbitrary natural number $n > 1$, then we still get a metric on $\mathbb{Z}$. Every non-zero integer z has a unique representation

$$z = n^i a,$$

where n does not divide a. We set

$$|z|_n := n^{-i} \quad \text{and} \quad |0|_n := 0.$$

Then $|\cdot|_n$ defines a metric. Note that $|\cdot|_n$ is not multiplicative as it is in the case $n = p$. We can form the completion $\mathbb{Z}_n$ with respect to that metric.

(d) Prove that $\mathbb{Z}_{10} \cong \mathbb{Z}_2 \times \mathbb{Z}_5$.

EX.2: DE RHAM COHOMOLOGY OF $\mathbb{C}$ MINUS m POINTS

Let $X := \mathbb{C} \setminus \{x_1, \dots, x_m\}$, where $x_1, \dots, x_m$ are distinct points in the complex plane, and let A be the set of rational functions, i.e. of the form g/h for polynomials $g, h \in \mathbb{C}[x]$ with $h \ne 0$, whose poles are contained in $\{x_1, \dots, x_m\}$. In algebraic language A is the ring of regular functions on X. There is a $\mathbb{C}$-linear map $D : A \to A$ given by $f \mapsto f' := df/dx$. It satisfies the Leibniz rule

$$D(gh) = gDh + hDg.$$

We set

$$H^1_{DR}(X) := A/DA,$$

where DA denotes the image of A under the map D.

(a) Explain why the elements

$$x^l \ ,\ l \ge 0 \quad \textbf{and} \quad \frac{1}{(x - x_j)^k} \ ,\ 1 \le j \le m \ ,\ k > 0$$

form a $\mathbb{C}$-basis of A.

(b) Prove that the quotient vectorspace $H^1_{DR}(X)$ has $\mathbb{C}$-dimension m by giving a suitable basis.

Note that A is the ring of meromorphic functions on the Riemann sphere $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$ being holomorphic on X.

Now let A be the ring of functions being holomorphic on X. (Essential singularities at the x_j and at ∞ are allowed.) We will prove that (with the notation from above) $H^1_{DR}(X)$ still has dimension m. Therefore we define a map $R : A \to \mathbb{C}^m$ by mapping

$$f \mapsto \left(\mathrm{Res}_{x_j} f\right)_{j=1,\dots,m}$$

where

$$\mathrm{Res}_{x_j} f := \frac{1}{2\pi i} \oint_{x_j} f dx$$

is the residue of f at x_j.

(c) Prove that

$$A \xrightarrow{D} A \xrightarrow{R} \mathbb{C}^m \to 0$$

is exact.
(Hint: Choose a point $x_0 \neq x_j$, $j = 1, \dots, m$. Set

$$F(z) := \int_{x_0}^{z} f dx.$$

When is this expression well-defined?)

We remark that the above statements remain true if we remove closed discs instead of points.

EX.3: POWER SERIES WITH COEFFICIENTS IN $\mathbb{Z}_p$

Let $p > 2$ and $|\cdot|_p$ as in EX.1. For $i \in \mathbb{N}$ we set

$$\binom{x}{i} := \frac{1}{i!} \prod_{n=0}^{i-1} (x - n) \in \mathbb{Q}[x].$$

One can evaluate this polynomial at rational numbers. A classical result is that $\binom{x}{i}$ is integer valued on $\mathbb{Z}$.

(a) Prove that $\binom{1/2}{i}$ has p-adic absolute value smaller or equal to 1 and conclude that the power series

$$F(x) := \sum_{i=0}^{\infty} \binom{\frac{1}{2}}{i} x^i$$

converges on the open unit disc in $\mathbb{Z}_p$, i.e. for $x \in \mathbb{Z}_p$ with $|x|_p < 1$.
(Hint: Consider the function $\mathbb{Z} \to \mathbb{Z}$, $x \mapsto \binom{x}{i}$. It is continuous with respect to $|\cdot|_p$. It can be extended to $\mathbb{Z}_p$.)

(b) Show that

$$F(x)^2 = 1 + x$$

in the ring of formal power series $\mathbb{Q}[[x]]$.
(Hint: If $F(x)^2 = 1 + x$ then $(1 + x)F'(x) = \frac{1}{2}F(x)$. This gives recursive formulas for the coefficients of F.)

(c) Compute an integer z such that $z^2 \equiv -2 \bmod 81$.
(Hint: Use the power series F.)

EX.4: EQUATIONS DEFINING HYPERELLIPTIC CURVES

Let $Q \in \mathbb{C}[x]$ be a separable polynomial of odd degree $d := 2g+1$, $g > 0$. Consider the affine curve C given by

$$y^2 = Q(x). \tag{2}$$

Since Q is separable, it is non-singular. We want to find a complete non-singular model. It is not possible to make such a model in $\mathbb{P}^2_{\mathbb{C}}$ except for the case $g = 1$.

(a) Complete the curve C by making a non-singular model at ∞ and a glueing morphism between C and the model at ∞.

(Hint: Set $t := 1/x$ and substitute $x = 1/t$ into equation (2). Introduce a second coordinate s such that the model at ∞ is of the form

$$s^2 = \text{polynomial in } t.$$

The glueing morphism is then given by $(x, y) \mapsto (t, s)$.)

We denote the completion of C by $\bar{C}$. Projecting on x and t we get a finite morphism $\bar{C} \to \mathbb{P}^1_{\mathbb{C}}$ of degree 2. A curve admitting such a morphism is called *hyperelliptic*.

(b) Show that $\bar{C}$ has genus g.
(Hint: Use the Hurwitz formula.)

EX.5: UNRAMIFIED EXTENSIONS OF $\mathbb{Q}_p$

Let p be a prime, $q := p^d$ and $f \in \mathbb{F}_p[x]$ an irreducible polynomial of degree d. Then $\mathbb{F}_q = \mathbb{F}_p[x]/(f)$ is a finite field having q elements. There is a surjective ring homomorphism $\mathbb{Z}_p \to \mathbb{F}_p$ given by $a \mapsto a \bmod p$. Now let $f_1, f_2 \in \mathbb{Z}_p[x]$ be monic polynomials such that $f_i \equiv f \bmod p$ and set $R_i := \mathbb{Z}_p[x]/(f_i)$. Since the f_i are irreducible, the rings R_i are integral domains. There are surjective reduction maps $\pi_i : R_i \to \mathbb{F}_q$.

(a) Show that there is a unique $\mathbb{Z}_p$-algebra homomorphism $\gamma : R_1 \to R_2$ such that $\pi_2\gamma = \pi_1$.
(Hint: We denote by $[x]$ the equivalence class of x in R_1. It is a zero of f_1. Lift the reduction of $[x]$ modulo p to a root of f_1 in R_2 using the completeness of R_2 and Newton's method.)

By $\mathbb{Z}_q$ we denote a $\mathbb{Z}_p$-algebra surjecting on $\mathbb{F}_q$, which is an integral domain and whose field of fractions has $\mathbb{Q}_p$-dimension d, for example take R_i. As we have proven above this is well-defined up to unique isomorphism. We denote the field of fractions of $\mathbb{Z}_q$ by $\mathbb{Q}_q$.

The next exercise is to prove that $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_q) = \mathrm{Aut}_{\mathbb{Z}_p}(\mathbb{Z}_q)\ \big[= \mathrm{Aut}_{\mathbb{Q}_p}(\mathbb{Q}_q)\big]$.

(b) Prove that the p-th power Frobenius f_p on $\mathbb{F}_q$ admits a lifting to R_i, i.e. a map $F_p \in \mathbf{End}_{\mathbb{Z}_p}(R_i)$ such that $\pi_i f_p = F_p \pi_i$.
(Hint: Modify the proof of (a).)

The proof of (b) gives an explicit method for computing the Frobenius action on $\mathbb{Q}_q$.

The lifting part can be done as a precomputation.

Terminology: We remark that a short way of characterizing $\mathbb{Q}_q$ is to say that it is the unramified extension of $\mathbb{Q}_p$ of degree d. The ring $\mathbb{Z}_q$ can also be described as the ring of p-Witt vectors with values in $\mathbb{F}_q$.