Homework 8

The homeworks are due on the Thursday of the week after the assignment was posted online[1]. Please hand in your homework at the beginning of the tutorial or bring it to the lecture on Thursday morning. You can work on and submit your homework in groups of two. Please staple your pages and write your names and matriculation numbers on the first page.

Problem 22 (10 pts.)

Let p be a prime number. Let $\overline{\mathbb{Q}}_p$ be the algebraic closure of $\mathbb{Q}_p$, i.e., the (up to isomorphism) unique algebraic extension K of $\mathbb{Q}_p$ that is algebraically closed. We can construct $\mathbb{Q}_p$ as the splitting field of all polynomials in $\mathbb{Q}_p[X]$ or, equivalently, the union of all finite extensions of $\mathbb{Q}_p$ (and then show that this is an algebraically closed field). We know that the algebraic closure of $\mathbb{R}$ is $\mathbb{C}$ and thus $\overline{\mathbb{R}}$ has degree 2 over $\mathbb{R}$.
Show that, however, the extension $\overline{\mathbb{Q}}_p/\mathbb{Q}_p$ is infinite.
Hint 1: Show that, for every $n \in \mathbb{N}$, there is an irreducible polynomial $f \in \mathbb{Q}_p[X]$ of degree n. For this you may use, for example, the reduction criterion for polynomials over a unique factorization domain and Hint 2.
Hint 2: Use the following fact from Algebra. For all $n \in \mathbb{N}$ there is a finite field $\mathbb{F}_{p^n}$ with p^n elements. The extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is a Galois extension of degree n.

Solution. The idea is to show that there are irreducible polynomials of arbitrarily large degrees over $\mathbb{Q}_p$. Since the root of an irreducible polynomial of degree n generates an extension of degree n, $\overline{\mathbb{Q}}_p$ will contain extensions of arbitrarily large degree n, and so it cannot be a finite extension.
We will use next Hint 2, which is a result from finite fields saying that, for every $n \geq 1$, the finite field $\mathbb{F}_p$ has a unique extension of degree n, which is the field $\mathbb{F}_{p^n}$ with p^n elements. The extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois, in particular separable, hence there exists a polynomial $f(X)$ such that $\mathbb{F}_{p^n}$ is obtained by adjoining a root of $f(X)$ to $\mathbb{F}_p$. In fact, this says that, for every $n \geq 1$, there is an irreducible polynomial of degree n in $\mathbb{F}_p[X]$ whose roots generate the unique extension $\mathbb{F}_{p^n}$. We finally use the following irreducibility criterion:
Let $f(X) \in \mathbb{Z}_p[X]$ be a monic polynomial whose reduction modulo p is irreducible in $\mathbb{F}_p[X]$. Then $f(X)$ is irreducible over $\mathbb{Q}_p$.
Choosing now any lift of the irreducible polynomial $f(X)$ to a monic polynomial in $\mathbb{Z}_p[X]$ gives an irreducible polynomial of degree n in $\mathbb{Q}_p[X]$, as desired. □

Problem 23 (10 pts.)

Let $K/\mathbb{Q}_p$ be a finite extension, $|\ |$ the unique extension of the p-adic absolute value to K. Let $\mathcal{O}_K \subset K$ be the valuation ring. Show that $\mathcal{O}_K$ consists exactly of those elements $x \in K$ that are roots of a monic polynomial with coefficients in $\mathbb{Z}_p$ (i.e., $\mathcal{O}_K$ is the "ring of integers" in K).

[1] This assignment is due Thursday, 05.12.19.

Solution. If $[K:\mathbb{Q}_p]=n$ and $\alpha\in\mathcal{O}_K$, then $|\alpha|=\sqrt[n]{|\mathrm{N}_{K/\mathbb{Q}_p}(\alpha)|_p}\leq 1$. But since the norm equals $(-1)^{r\deg f}a_0^r$, where a_0 is the constant term of the minimal polynomial f of α and $r=[K:\mathbb{Q}_p(\alpha)]$, this means that $|a_0|_p\leq 1$ and so $a_0\in\mathbb{Z}_p$. It then follows, by a corollary from Hensel seen in class (Kor. 2.1), that f has coefficients in $\mathbb{Z}_p$. Conversely, consider any x whose minimal polynomial $f(X)=X^n+\cdots+a_1X+a_0$ has coefficients in $\mathbb{Z}_p$. Then

$$|x|_p^n=|a_{n-1}x^{n-1}+\cdots+a_1x+a_0|_p\leq\max_{1\leq i\leq n-1}|a_ix^i|_p\leq\max_{1\leq i\leq n-1}|x|_p^i\quad(\text{since }|a_i|_p\leq 1),$$

which implies $|x|_p\leq 1$. Alternatively one can use Lemma 2.2 from the Script. □

Problem 24 (10 pts.)

Let $e=e(K/\mathbb{Q}_p)$ be the *ramification index* as defined in Exercise 26. If we write $f=f(K/\mathbb{Q}_p)=n/e$ and if $\Bbbk=\mathcal{O}/\mathfrak{p}$ denotes the residue field, then $[\Bbbk:\mathbb{F}_p]=f$, so that $\Bbbk=\mathbb{F}_{p^f}$ is the finite field with p^f elements. You don't need to prove this! Instead, just try to exemplify this result by computing e,f and n for the following two fields:

(i) $p=5,\ K=\mathbb{Q}_5(\sqrt{2})$.

(ii) $p=5,\ K=\mathbb{Q}_5(\sqrt{5})$.

(iii) $p=5,K=\mathbb{Q}_5(\sqrt{11})$.

(iv) **Bonus (5 pts.)**: $p=3,\ K=\mathbb{Q}_3(\zeta,\sqrt{2})$, where ζ is a primitive third root of unity, i.e., $\zeta^3=1$ but $\zeta\neq 1$.

Solution. (i) We have seen in Exercise 26 that $e=1$ and that $n=2$. Therefore, we need to show that $f=2$. We can compute $\mathcal{O}$ either directly, or by invoking the result from Problem 23. In either case, the answer is $\mathcal{O}=\mathbb{Z}_5[\sqrt{2}]$. We have $\mathcal{O}=\{x\in K:|x|_5\leq 1\}$. But if $x=a+b\sqrt{2}$ with $a,b\in K$, then $|x|_5=\sqrt{|\mathrm{N}_{K/\mathbb{Q}_5}(x)|_5}=\sqrt{|a^2-2b^2|_5}$, and $|x|_5\leq 1$ implies $|a^2|_5,|b^2|_5\leq 1$, from where it follows indeed that $\mathcal{O}=\mathbb{Z}_5[\sqrt{2}]$. To compute the maximal ideal $\mathfrak{p}$ we need $|x|_5<1$, hence $\mathfrak{p}=5\mathbb{Z}_5[\sqrt{2}]$ and $\Bbbk=\mathbb{F}_5[\sqrt{2}]$, thus $f=[\Bbbk:\mathbb{F}_5]=2$. (ii) It is clear that 5 itself is not a square in $\mathbb{Q}_5$ and that $K=\mathbb{Q}_5(\sqrt{5})$ is an extension of degree 2 with $\{1,\sqrt{5}\}$ a basis. Hence $e\in\{1,2\}$. If $x=\sqrt{5}$, we have $\nu_5(x)=\frac{1}{2}$, hence we must have $e=2$ and we need to prove that $f=1$, for which we need to show that $\Bbbk=\mathbb{F}_5$. Just like before, we have $\mathcal{O}=\mathbb{Z}_5[\sqrt{5}]$. To compute $\mathfrak{p}$, we need $|x|_5=\sqrt{|a^2-5b^2|_5}<1$, which holds iff $a\in 5\mathbb{Z}_5$ and $b\in\mathbb{Z}_5$ and which gives $\mathfrak{p}=(\sqrt{5})=5\mathbb{Z}_5\oplus\sqrt{5}\mathbb{Z}_5$ and $\Bbbk=\mathbb{F}_5$ indeed. (iii) The trick here is that $11\equiv 1\pmod 5$ and $\left(\frac{1}{5}\right)=1$, therefore 11 is a square in $\mathbb{Q}_5$ and $K=\mathbb{Q}_5$, so there is nothing to do here: $e=f=n=1$. (iv) K is an extension of degree 4 over $\mathbb{Q}_p$, hence $n=4$ (both $\mathbb{Q}_3(\zeta)$ and $\mathbb{Q}_3(\sqrt{2})$ are subextensions of degree 2). Thus $e\in\{1,2,4\}$. We claim that $e=2$. It is not hard to see, on recalling that $1+\zeta+\zeta^2=0$, that $x=1-\zeta$ is a uniformizer in K. Let's compute its norm. Since $[K:\mathbb{Q}_3(\zeta)]=2$, we have

$$\begin{aligned}\mathrm{N}_{K/\mathbb{Q}_3}(1-\zeta)&=\mathrm{N}_{\mathbb{Q}_3(\zeta)/\mathbb{Q}_3}(\mathrm{N}_{K/\mathbb{Q}_3(\zeta)}(1-\zeta))\\&=\mathrm{N}_{\mathbb{Q}_3(\zeta)/\mathbb{Q}_3}(1-\zeta)^2.\end{aligned}$$

To compute this last norm, regard $\mathbb{Q}_3(\zeta)$ as a 2-dimensional vector space over $\mathbb{Q}_3$ with basis $\{1,\zeta\}$. The matrix of multiplication by $1-\zeta$ is $\begin{pmatrix}1&1\\-1&2\end{pmatrix}$ and so the norm, which is just the determinant of this matrix, is equal to 3, which gives $\nu_3(x)=\frac{1}{4}\nu_3(9)=\frac{1}{2}$, from where we conclude that $e = 2$. Finally, we need to show that $f = 2$. It is not hard to see that $\mathcal{O} = \mathbb{Z}_3[\zeta, \sqrt{2}]$ and we know that $\mathfrak{p} = (1 - \zeta)$, from where we infer that $\Bbbk = \mathbb{Z}_3[\zeta, \sqrt{2}]/(1 - \zeta) = \mathbb{F}_3[\sqrt{2}]$, thus $f = [\Bbbk : \mathbb{F}_3] = 2$. □

The following exercises will be discussed in the tutorial and you do not need to hand in solutions for them.

Exercise 25

Let $p = 5$. Check that 2 is not a square in $\mathbb{Q}_5$ and consider the quadratic extension $K = \mathbb{Q}_5(\sqrt{2})$. View K as a 2-dimensional $\mathbb{Q}_5$-vector space and give an example of a (vector space) norm on K that is not a valuation on K but does extend the p-adic absolute value on $\mathbb{Q}_5$.

Solution. This should be clear by now, as quadratic residues mod 5 are only $0, 1, 4$. An example of such a norm is given by $\|a + b\sqrt{2}\| = \sqrt{|a|_5^2 + |b|_5^2}$. This gives the 5-adic norm $|\ |_5$ when $b = 0$, i.e., when restricted to $\mathbb{Q}_5$, but is not a valuation on K. This is so because the multiplicativity property of a valuation is not satisfied:

$$\|a + b\sqrt{2}\|\|c + d\sqrt{2}\| = \sqrt{|ac + 2bd|_5^2 + |ad + bc|_5^2}, \tag{1}$$

while

$$\sqrt{|a|_5^2 + |b|_5^2}\sqrt{|c|_5^2 + |d|_5^2} = \sqrt{(|a|_5^2 + |b|_5^2)(|c|_5^2 + |d|_5^2)}. \tag{2}$$

But by the strong triangle inequality, $|ac + 2bd|_5^2 \leq \max\{|ac|_5^2, |bd|_5^2\}$ (the factor 2 does not contribute to the 5-adic valuation), while $|ad + bc|_5^2 \leq \max\{|ad|_5^2, |bc|_5^2\}$. In any case, the expression from (1) will be strictly smaller than that from (2) for $a, b, c, d \neq 0$. □

Exercise 26

Let $K/\mathbb{Q}_p$ be a finite extension of degree n. Let v be the unique extension of the p-adic valuation v_p to K.

(a) Show that there is a positive integer $e \geq 1$, such that $e \mid n$ and

$$v(K^\times) = \frac{1}{e}\mathbb{Z}.$$

This integer is called the *ramification index* of $K/\mathbb{Q}_p$.

(b) Let $K = \mathbb{Q}_5(\sqrt{2})$, which is a quadratic extension of $\mathbb{Q}_5$. Find the ramification index $e = e(K/\mathbb{Q}_5)$ in this example.

Solution. (a) Recall that $\nu(x) = \frac{1}{n}\nu_p(\mathrm{N}_{K/\mathbb{Q}_p}(x))$. This implies that $\nu(K^\times) \subset \frac{1}{n}\mathbb{Z}$. By the property that $\nu(xy) = \nu(x) + \nu(y)$, we conclude that $\nu(K^\times)$ is an additive subgroup of $\frac{1}{n}\mathbb{Z}$. Now let d/e be in the image $\nu(K^\times)$, with $(d, e) = 1$, chosen such that e is the largest denominator that occurs. This is possible since it is clear that $e \mid n$, so that the range of possible denominators is bounded. As $(d, e) = 1$, one finds integers r, s such that $rd - se = 1$, thus

$$r\frac{d}{e} = \frac{1 + se}{e} = \frac{1}{e} + s$$

is in the image. Since $s \in \mathbb{Z}$ is in the image, it follows that $1/e$ is also in the image. But then it follows that the image must be exactly $\frac{1}{e}\mathbb{Z}$, as e was chosen to be the largest possible

denominator.
(b) This can be done in the simplest way: we know that $\nu_p(x) = \frac{1}{2}\nu_p(\mathrm{N}_{K/\mathbb{Q}_p}(x))$ for any $x \in \mathbb{Q}_5(\sqrt{2})$. But any such x is of the form $x = a + b\sqrt{2}$, with $a, b \in \mathbb{Q}_5$. Then we compute $\mathrm{N}_{K/\mathbb{Q}_p}(x) = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$, and we notice that the valuation of 5 in $a^2 - 2b^2$ must be even. If $\nu_5(a^2) \neq \nu_5(b^2)$, this is clear as $(2, 5) = 1$ and so $\nu_5(a^2 - 2b^2) = \min\{\nu_5(a^2), \nu_5(b^2)\}$, which is an even number. Otherwise, as long as a^2 and $2b^2$ do not start with the same 5-adic digit, the result still holds. But this cannot happen as 2 is not a quadratic residue mod 5. This implies that the image of $\nu_p(x)$ is always in $\mathbb{Z}$, hence $e = 1$. □