MIDTERM EXAM

MATH-GA 2210.001 ELEMENTARY NUMBER THEORY

Each problem will be marked out of 20 points.

Problem 1. Find the p-adic expansions for

(1) $\frac{2}{3}$ in $\mathbb{Q}_2$,
(2) $-\frac{1}{6}$ in $\mathbb{Q}_7$,
(3) $\frac{1}{10}$ in $\mathbb{Q}_{11}$,
(4) $\frac{1}{120}$ in $\mathbb{Q}_5$.

`Solution.`

(1) In $\mathbb{Q}_2$, we have
$$\frac{2}{3} = \sum_{i=0}^{\infty} a_i 2^i,$$
where $a_n \in \{0,1\}$. Then we have the recurrence relation
$$f_{n-1} = 3a_{n-1} + 2f_n,$$
where $f_n \in \mathbb{Z}$, and $f_0 = 2$. Since each iteration has a unique solution, we simply solve for the sequences
$$\begin{aligned} f_1 &= 1 & a_0 &= 0 \\ f_2 &= -1 & a_1 &= 1 \\ f_3 &= -2 & a_2 &= 1 \\ f_4 &= -1 & a_3 &= 0 \\ f_5 &= -2 & a_4 &= 1 \\ &\vdots & &\vdots \end{aligned}$$
We see that the sequences beginning with f_3 and a_2 will be periodic. So, this means that we can write the 2-adic expansion
$$\frac{2}{3} = 2 + 2^2 + 2^4 + 2^6 + 2^8 + \cdots$$
(2) In $\mathbb{Q}_7$, we have
$$-\frac{1}{6} = \frac{1}{1-7} = 1 + 7 + 7^2 + 7^3 + \cdots$$
Or like above, we could solve the recurrence relation
$$f_{n-1} = 6a_{n-1} + 7f_n,$$

This take home exam is due on Wednesday 4 March 2015.

where $f_n \in \mathbb{Z}$, $a_n \in \{0, 1, \ldots, 6\}$, and $f_0 = -1$. This gives $a_n = 1$ and $f_n = -1$ for all n.

(3) We have to find the 11-adic expansion for $\frac{1}{10}$. Similarly to above, we have to solve the recurrence relation

$$f_{n-1} = 10a_{n-1} + 11f_n,$$

where $f_n \in \mathbb{Z}$, $a_n \in \{0, 1, \ldots, 10\}$, and $f_0 = 1$. Since each iteration has a unique solution, we simply solve for the sequences

$$\begin{aligned} f_1 &= -9 & a_0 &= 10 \\ f_2 &= -9 & a_1 &= 9 \\ f_3 &= -9 & a_2 &= 9 \\ &\vdots & &\vdots \end{aligned}$$

We see that the sequences beginning with f_2 and a_1 will be periodic, and

$$\frac{1}{10} = 10 + 9(11) + 9(11)^2 + 9(11)^3 + \cdots$$

(4) In $\mathbb{Q}_5$, we have

$$\frac{1}{120} = \frac{1}{5}\frac{1}{24}.$$

Let us find the 5-adic expansion of $\frac{1}{24}$. We want to solve the recurrence relation

$$f_{n-1} = 24a_{n-1} + 5f_n,$$

where $f_n \in \mathbb{Z}$, $a_n \in \{0, 1, 2, 3, 4\}$, and $f_0 = 1$. Since each iteration has a unique solution, we simply solve for the sequences

$$\begin{aligned} f_1 &= -19 & a_0 &= 4 \\ f_2 &= -23 & a_1 &= 4 \\ f_3 &= -19 & a_2 &= 3 \\ f_4 &= -23 & a_3 &= 4 \\ &\vdots & &\vdots \end{aligned}$$

We see that the sequences beginning with f_2 and a_1 will be periodic. So, this means that we can write the 5-adic expansion

$$\frac{1}{120} = \frac{1}{5}\frac{1}{24} = \frac{4}{5} + 4 + 3(5) + 4(5)^2 + 3(5)^3 + 4(5)^4 + \cdots$$

Problem 2. Prove that the the field $\mathbb{Q}_p$ does not have automorphisms except the identity.

`Solution.` Let $\sigma \colon \mathbb{Q}_p \to \mathbb{Q}_p$ be an automorphism. Then it takes $1 \mapsto 1$, since σ is an automorphism. Since 1 generates $\mathbb{Q}$, we see that $x \mapsto x$ for all $x \in \mathbb{Q}$.

Let us show that σ is continuous. This follows from the fact that σ preserves the valuation (i.e., we must have $|\sigma(x)|_p = |x|_p$ for every $x \in \mathbb{Q}_p$). Let us show the latter. Observe that the composition of σ with the p-adic valuation,

$$\big|\sigma(\quad)\big|_p : \mathbb{Q}_p \to \mathbb{R}$$

is itself a valuation, because σ is a field homomorphism. Moreover, this valuation agrees with $|\quad|_p$ on $\mathbb{Q}$. Let $\{s_n\}$ be a cauchy sequence in $\mathbb{Q}$. Then it converges with respect to $|\quad|_p$ to some limit s. We want to show that it converges to a limit in $\mathbb{Q}_p$ with respect to the valuation $|\sigma(\quad)|_p$ to $\sigma^{-1}(s)$. Fix some $\epsilon > 0$. Since $s_n \to s$ in $(\mathbb{Q}_p, |\quad|_p)$, we know that

$$\big|s - s_n\big| < \epsilon$$

for sufficiently large $n > N$. This implies

$$\Big|\sigma\big(\sigma^{-1}(s) - s_n\big)\Big|_p = \big|s - \sigma(s_n)\big|_p = |s - s_n|_p < \epsilon$$

for $n > N$, because σ is a field homomorphism and it is the identity map on $s_n \in \mathbb{Q}$. Thus, $\{s_n\}$ converges in $(\mathbb{Q}_p, |\sigma(\quad)|_p)$, so that $\mathbb{Q}_p$ is complete with respect to this valuation. And if $|\sigma(\quad)|_p$ is a complete extension of $|\quad|_p$ to $\mathbb{Q}_p$, it must be equal to $|\quad|_p$ since we know such extensions are unique. So σ is continuous.

Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$ (by the construction of $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$ with respect to the p-adic valuation), we see that σ is an identity map on a dense subset of $\mathbb{Q}_p$. Hence, σ is an identity map, because we already proved that σ is the identity on $\mathbb{Q}$, and σ is continuous.

Problem 3. Prove that

(1) the polynomial $x^2 - 5$ is irreducible in $\mathbb{Q}_7[x]$,
(2) the polynomial $x^p - x - 1$ is irreducible in $\mathbb{Q}_p[x]$ for any prime $p \geqslant 2$,
(3) the polynomial $x^4 + 4x^3 + 2x^2 + x - 6$ is reducible in $\mathbb{Q}_{11}[x]$,
(4) the polynomial $x^4 - x^3 - 2x^2 - 3x - 1$ is reducible in $\mathbb{Q}_5[x]$.

`Solution.` Prove that

(1) Suppose we had a root $\alpha = 7^{-m}a$ such that $\alpha^2 - 5 = 0$ for $a \in \mathbb{Z}_7^*$. Then this implies $7^{-2m}|5$, which can only happen if $m = 0$. So we know that any solution α must be in $\mathbb{Z}_7$. However, if such a root existed, we would have a root in $\mathbb{F}_7$. But we can easily check 5 is not a square in $\mathbb{F}_7$, because only 1, 2 and 4 are squares. So this polynomial is irreducible over $\mathbb{Q}_7$.
(2) Suppose that $x^p - x - 1$ is reducible in $\mathbb{Q}_p[x]$ for some prime $p \geqslant 2$. Then $x^p - x - 1$ is reducible in $\mathbb{Z}_p[x]$ by Gauss' lemma. Reducing mod p, we see that $x^p - x - 1$ is reducible in $\mathbb{F}_p[x]$. So, we have

$$x^p - x - 1 = f(x)g(x)$$

for some polynomials $f(x)$ and $g(x)$ in $\mathbb{F}_p[x]$ such that $f(x)$ is irreducible, and both $f(x)$ and $g(x)$ are of positive degree. Denote the degree of $f(x)$ by d. Then $d < p$ by assumption. Moreover, $d > 1$, because the polynomial $x^p - x - 1$ does not have roots in $\mathbb{F}_p$ (this follows from Fermat's Little Theorem). Denote by K the field

$$\mathbb{F}_p[x]/(f(x)),$$

where $(f(x))$ is the ideal generated by $f(x)$. Then K is a field extension of $\mathbb{F}_p$ of degree d. Thus, it contains p^d elements. Then

$$\alpha^{p^d-1} = 1$$

for every $\alpha \in K^*$ by Lagrange's theorem. Thus, we have $\alpha^{p^d} = \alpha$ for every $\alpha \in K$. In particular, we have

$$\bar{x}^{p^d} = \bar{x},$$

where $\bar{x} \in K$ is the image of $x \in \mathbb{F}_p[x]$ under natural projection $\mathbb{F}_p[x] \to K$. On the other hand, we have

$$\bar{x}^{p^c} = \bar{x} + c$$

for every $c \in \mathbb{Z}_{\geqslant 0}$. Indeed, we can prove it by induction. For $c = 0$, this is true. If it is true for some $c \geqslant 0$, we have

$$\bar{x}^{p^{c+1}} = \left(\bar{x} + c\right)^p = \bar{x}^p + c^p = \bar{x} + 1 + c^p = \bar{x} + 1 + c,$$

because $\bar{x}^p = \bar{x} + 1$ in K, and $c^p = c$ by Fermat's Little Theorem. This proves that $\bar{x}^{p^c} = \bar{x} + c$ for every $c \in \mathbb{Z}_{\geqslant 0}$. In particular,

$$\bar{x} = \bar{x}^{p^d} = \bar{x} + d,$$

which implies that $d = 0$ in K. The latter is impossible, since $d < p$.

(3) Put $f(x) = x^4 + 4x^3 + 2x^2 + x - 6$. Let us show that $f(x)$ is reducible in $\mathbb{Q}_{11}[x]$. Observe that

$$x^4 + 4x^3 + 2x^2 + x - 6 \equiv (x+4)(x^3 + 2x + 4) \bmod 11.$$

Moreover, the polynomials $x + 4$ and $x^3 + 2x + 4$ are co-prime in $\mathbb{F}_{11}[x]$. Thus, it follows from Hensel's lemma (see [1, Lemma II.4.6]) that $f(x)$ splits as a product of a polynomial of degree 1 and a polynomial of degree 3 in $\mathbb{Z}_{11}[x]$.

(4) We have

$$x^4 - x^3 - 2x^2 - 3x - 1 = (x^2 + x + 1)(x^2 - 2x - 1)$$

in $\mathbb{F}_5[x]$. Moreover, the polynomials $x^2 + x + 1$ and $x^2 - 2x - 1$ are coprime in $\mathbb{F}_5[x]$. Arguing as above, we see that the polynomials $x^4 - x^3 - 2x^2 - 3x - 1$ is a product of two quadratic polynomials in $\mathbb{Z}_5[x]$.

Problem 4. Show that for every $d \in \mathbb{N}$, there is a field K containing $\mathbb{Q}_p$ such that

$$[K : \mathbb{Q}_p] := \dim_{\mathbb{Q}_p}(K) = d.$$

`Solution.` We know that there exists a field $\mathbb{F}_{p^d}$ consisting of p^d elements. It can be constructed from $\mathbb{F}_p$ by adding all roots of the polynomial $x^{p^d} - x \in \mathbb{F}_p[x]$, which also show that the field consisting of p^d is unique. Note that the extension $\mathbb{F}_p \subset \mathbb{F}_{p^d}$ is separable, since the derivative of $x^{p^d} - x$ is not a zero polynomial. Hence, $\mathbb{F}_{p^d} = \mathbb{F}_p(\alpha)$ for some $\alpha \in \mathbb{F}_{p^d}$. Let $f(x) \in \mathbb{F}_p[x]$ be the minimal polynomial of α. Then it is irreducible and of degree d. Let $g(x)$ be any polynomial of degree d in $\mathbb{Z}_p[x]$ such that

$$g(x) \equiv f(x) \bmod p.$$

Then $g(x)$ is irreducible in $\mathbb{Z}_p[x]$. By Gauss' lemma, it is irreducible in $\mathbb{Q}_p[x]$. Adding its root to $\mathbb{Q}_p$, we obtain a field K containing $\mathbb{Q}_p$ such that

$$[K : \mathbb{Q}_p] := \dim_{\mathbb{Q}_p}(K) = d$$

as desired.

Problem 5. Let K be the field of fractions of the ring

$$\mathbb{Q}_7[x]/(x^2 - 5),$$

where $(x^2 - 5)$ is the ideal in $\mathbb{Q}_7[x]$ generated by $x^2 - 5$. Identify $\mathbb{Q}_7$ with a subfield of K via natural homomorphisms

$$\mathbb{Q}_7 \hookrightarrow \mathbb{Q}_7[x] \to \mathbb{Q}_7[x]/(x^2 - 5) \hookrightarrow K$$

Prove that the p-adic valuation $|\quad|_7$ on $\mathbb{Q}_7$ can be extended to a valuation

$$|\quad| \colon K \to \mathbb{R}_{\geqslant 0}$$

of the field K in a unique way. Describe its valuation ring

$$\mathcal{O} := \Big\{ x \in K \text{ such that } |x| \leqslant 1 \Big\},$$

its unique maximal ideal $\mathfrak{I}$, its residue class field $\mathcal{O}/\mathfrak{I}$, and its multiplicative group K^*.

`Solution.` To show that the valuation extends uniquely, all we need to do is show that K is algebraic over $\mathbb{Q}_7$. This follows from the fact that $x^2 - 5$ is irreducible over $\mathbb{Q}_7$ (see Problem 3).

For this particular extension, we see that $\sqrt{5}$ must be a unit, since $5 \in \mathbb{Z}_7^*$, and the valuation is multiplicative. We claim that the valuation ring is exactly

$$\mathcal{O} = \Big\{ a + b\sqrt{5} \;\Big|\; a, b \in \mathbb{Z}_p \Big\}.$$

That is, either a or b is in $\mathbb{Z}_7$. This follows immediately from the fact that since $a \neq b\sqrt{5}$, we have

$$\big|a + b\sqrt{5}\big|_7 = \max\Big\{ \big|a\big|_7, \big|b\sqrt{5}\big|_7 \Big\} = \max\big\{ |a|_7, |b|_7 \big\},$$

so that $|a + b\sqrt{5}|_7 \leq 1 \Leftrightarrow a, b \in \mathbb{Z}_7$.

By the same reasoning, we see that it's unique maximal ideal $\mathfrak{I}$ is just

$$\mathfrak{I} = \Big\{ a + b\sqrt{5} \;\Big|\; a, b \in \mathfrak{p} \Big\},$$

where $\mathfrak{p}$ is the maximal ideal in $\mathbb{Z}_7$ generated by 7. In particular, as an additive group we have $\mathfrak{J} \cong \mathbb{Z}_7^2$.

If we recall that the residue class field of $\mathbb{Q}_7$ is $\mathbb{F}_7$, we see that we can take the quotient to find

$$\mathcal{O}/\mathfrak{J} \cong \mathbb{F}_7[\sqrt{5}] \cong \mathbb{F}_{49},$$

i.e., all elements of the form $a + b\sqrt{5}$, where $a, b \in \mathbb{F}_7$.

Since $[K : \mathbb{Q}_7] = \deg(x^2 - 5) = 2$, it follows from [1, Proposition II.5.7], that there exists a natural number a such that the multiplicative group can be decomposed into

$$K^* \cong \mathbb{Z} \oplus \mathbb{Z}/48\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^2.$$

To find a, let us use [1, Proposition II.5.5]. It implies that the function

$$\log\colon K^* \to K$$

induces an isomorphism $\mathfrak{J}^n \to U^{(n)}$ for $n > \frac{1}{7-1} = \frac{1}{6}$. Thus, we have an isomorphisms of groups $\mathfrak{J} \cong U^{(1)}$. On the other hand, we already proved that $\mathfrak{J} \cong \mathbb{Z}_7^2$. Thus, we have $U^{(1)} \cong \mathbb{Z}_7^2$. But

$$K^* \cong \mathbb{Z} \oplus \mathbb{Z}/48\mathbb{Z} \oplus U^{(1)}$$

by [1, Proposition II.5.5]. This gives $a = 0$.

References

[1] J. Neukirch, *Algebraic Number Theory*, Springer, 1999.