Prof. Dr. Y. Tian
Dr. J. Anschütz

WS 2017/18

Algebraic Number Theory

9. Exercise sheet

Exercise 1 (4 Points):

Let p be an odd prime.

1. Prove that for any integer a with $1 \leq a \leq p-1$, there exists a unique $(p-1)$-th root of unity $u_a \in \mathbb{Z}_p$ such that $u_a \equiv a \bmod p$.

2. For any integer $n \geq 1$, let $n = a_0 + a_1 p + \ldots + a_r p^r$ be the p-adic expansion of n with $0 \leq a_i \leq p-1$. Put $s_p(n) = \sum_{i=0}^{r} a_i$. Prove that $v_p(n!) = \frac{n - s_p(n)}{p-1}$.

3. Prove that for any $x \in \mathbb{Z}_p$, the series
$$(1+p)^x := 1 + \sum_{n=1}^{\infty} \frac{x(x-1)\cdots(x-n+1)}{n!} p^n$$
converges to an element in $\mathbb{Z}_p$, and we have $(1+p)^{x+y} = (1+p)^x (1+p)^y$.

4. Prove that $\phi \colon x \mapsto (1+p)^x$ defines an isomorphism of abelian groups $(\mathbb{Z}_p, +) \cong (1 + p\mathbb{Z}_p, \times)$, and conclude that $\mathbb{Z}_p^\times = \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$.
Hint: To solve the equation $(1+p)^x = 1 + ap$ with $a \in \mathbb{Z}_p$, prove by induction on $n \geq 1$ that there exists $x_n \in \mathbb{Z}_p$ such that $(1+p)^{x_n} \equiv 1 + pa$ mod $(1 + p^n \mathbb{Z}_p)$, and that $(x_n)_{n \geq 1}$ is a Cauchy sequence in $\mathbb{Z}_p$.

Exercise 2 (4 Points):

Let K be a field complete with respect to a non-archimedean absolute value, $\mathcal{O} \subseteq K$ be its valuation ring. Let $f(X) \in \mathcal{O}[X]$ and $\alpha_0 \in \mathcal{O}$ with $|f(\alpha_0)| < |f'(\alpha_0)|^2$. Using the Newton iteration $\alpha_n = \alpha_{n-1} - \frac{\alpha_{n-1}}{f'(\alpha_{n-1})}$ prove that there exists a unique $\alpha \in \mathcal{O}$ with $f(\alpha) = 0$ and
$$|\alpha - \alpha_0| \leq \frac{|f(\alpha_0)|}{|f'(\alpha_0)|} < |f'(\alpha_0)| \leq 1.$$

Exercise 3 (4 Points):

1. Let p be a prime, and $n \geq 1$ be an integer with $p \nmid n$. Prove that for any $u \in \mathcal{O}_K^\times$, the equation $x^n = u$ has solutions in $\mathbb{Z}_p$ if and only it has solutions in $\mathbb{F}_p$.

2. Let p be an odd prime. Prove that $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

3. Prove that $\mathbb{Q}_2^\times / (\mathbb{Q}_2^\times)^2 \cong (\mathbb{Z}/2\mathbb{Z})^3$.

Exercise 4 (4 Points):

Using Newton polygons prove that the following polynomial is irreducible in $\mathbb{Q}[X]$:
$$f(x) = \sum_{n=0}^{10} \frac{x^n}{n!}.$$

To be handed in: Monday, 18. Dezember 2017.