Algebraická teorie čísel ZS 2020/21
Algebraic Number theory - fall term, 2020/21

Topic: not the standard ANT which deals with the arithmetic of number fields K ($K = \mathbb{Q}(\alpha)$, $\alpha \in \mathbb{C}$ is algebraic over $\mathbb{Q}$, is a finite algebr extension of $\mathbb{Q}$ $\Leftrightarrow$ $\mathbb{Q} \subset K$ is an extension of fields and K as a vector space over $\mathbb{Q}$ has finite dimension).

The topic of this course is Dwork's theorem on #s of sol-s of an equation over finite fields. Web resources: T. Tao wrote on this nicely, easy to google out. But we/I will follow the book Neal Koblitz, p-adic numbers, p-adic Analysis, and Zeta-Functions, Springer, New York, namely, Chapter V of it 1984.

First we have to give a precise statement of Dwork's theorem. So, at p. 113 of Koblitz's book, we can read.

Theorem⁰ (Dwork) The zeta-function of any affine (or projective - see Exercise 5 below) hypersurface is a ratio of two polynomials with coefficients in $\mathbb{Q}$ (actually, with coefficients in $\mathbb{Z}$ and constant term 1 - see Exercise 13 below).

---

this theorem was proven in the article:
B. Dwork, On the rationality of the zeta function of an algebraic variety, Amer. J. Math., 82 (1960), 631-648. We remark that J has >90 citations in MR (Mathematical Reviews) and that Bernhard Dwork (1923-1998) was an American mathematician, a (Ph.D.) student of Emil Artin (1898-1962) (who studied and lived before WWI in Reichenberg (or Liberec). See the article by N. M. Katz and J. Tate on B. Dwork, available on-line.

So let's turn to explaining the terms in the statement of Dwork's theorem.

• a variation of two polynomials.

Let $R=(R, 0_R, 1_R, +, \cdot)$ be a ring, commutative with $1_R (\neq 0_R)$. Then we can form the ring $R[\![x]\!]$ of formal power series with coefficients in R: $S := R[\![x]\!] := \{\sum_{n=0}^{\infty} a_n x^n \mid a_n \in R\}$, with the neutral elements $0_S := 0_R x^0 + 0_R x^1 + 0_R x^2 + \dots$ and $1_S := 1_R x^0 + 0_R x^1 + 0_R x^2 + \dots$, and operations $+$ and $\cdot$, given as

$$\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n := \sum_{n=0}^{\infty} (a_n + b_n) x^n$$

($+$ in S; $+$ in R)

$$\sum_{n=0}^{\infty} a_n x^n \cdot \sum_{n=0}^{\infty} b_n x^n := \sum_{n=0}^{\infty} \left(\sum_{q=0}^{n} a_q \cdot b_{n-q} \right) x^n$$

($\cdot$ in S; Cauchy prod.; $\cdot$ in R)

It is easy to show that $(R[\![x]\!], 0_S, 1_S, +, \cdot)$ is a ring again (comm., with 1_S).

Recall that $a \in R$ is <u>a unit</u> (in R) if there is $b \in R$ s.t. $ab = 1_R$. Let $U_R := \{\text{the units of } R\}$, then $(U_R, 1_R, \cdot)$ is an Abelian group, <u>the group of units of R</u>. What are the units in $R[[x]]$?

Proposition 1 $f(x) = \sum_{n=0}^{\infty} a_n x^n \in R[[x]]$ is a unit in $R[[x]] \iff a_0$ is a unit in R.

Proof.

$\Rightarrow$: $\sum_{n=0}^{\infty} a_n x^n \cdot \sum_{n=0}^{\infty} b_n x^n = 1_R x^0 + 0_R x + 0_R x^2 + \ldots \rightsquigarrow a_0 b_0 = 1_R$

$\sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) x^n$ $\rightsquigarrow a_0$ is a unit in R.

$\Leftarrow$: Suppose that $a_0 b_0 = 1_R$ for some $b_0 \in R$. We want to solve the system of ∞ many equations $\sum_{k=0}^{n} a_k b_{n-k} = \begin{cases} 1_R \ldots n = 0 \\ 0_R \ldots n > 0 \end{cases}$, $n = 0, 1, 2, \ldots$, in the unknown $b_n \in R$; the $a_n \in R$ are given. So $a_0 b_0^2 = 1_R \rightsquigarrow \underline{b_0 := b}$, $a_0 b_1 + a_1 b_0 = 0_R \rightsquigarrow \underline{b_1 := -a_1 b^2}$, $a_0 b_2^2 + a_1 b_1 + a_2 b_0 = 0_R \rightsquigarrow$

$b_2 := -b(a_1 b_1 + a_2 b_0) = \underline{a_1 b^3 - a_2 b^2}$, and so on, in this way we can solve, one by one, all equations and determine $b_0, b_1, b_2, \ldots$ ☒

---

the zeta function in Dwork's theorem in fact is not a function but an element $f(t) \in \mathbb{Z}[[t]]$, $f(t) = \sum_{n=0}^{\infty} a_n t^n$ with $a_n \in \mathbb{Z}$. the claim that $f(t)$ is a ratio of two polynomials means that $f(t) = \frac{P(t)}{Q(t)} = P(t) \cdot Q(t)^{-1}$ in $\mathbb{Q}[[t]]$, $P, Q \in \mathbb{Q}[t] \subset \mathbb{Q}[[t]]$ or in $\mathbb{Z}[[t]]$, $P, Q \in \mathbb{Z}[t] \subset \mathbb{Z}[[t]]$.

---

where $Q(t)^{-1} \in \mathbb{Q}[[t]]$, or $\in \mathbb{Z}[[t]]$, is the mult. inverse to the unit $Q(t)$; so $Q(t) \cdot Q(t)^{-1} = 1$. Thus $Q(0) \neq 0$ in $\mathbb{Q}[[t]]$ (units of $\mathbb{Q}$ are $\mathbb{Q} \setminus \{0\}$) or $Q(0) = \pm 1$ in $\mathbb{Z}[[t]]$ ($U_{\mathbb{Z}} = \{-1, 1\}$). this is the explanation of the "a ratio" in Dwork's thm.