CONGRUENT ZETA FUNCTIONS. NO.2

YOSHIFUMI TSUCHIMOTO

In this lecture we define and observe some properties of conguent zeta functions.

existence of finite fields II.

For any prime p, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. To construct $\mathbb{F}_{p^r}$ for r,

(1) We find an irreducible polynomial $u(X) \in \mathbb{F}_p[X]$ of degree r. (Such a thing exists always.)
(2) $K = \mathbb{F}_p[X]/(u(X))$ is a field with p^r elements. It is an extension field of $\mathbb{F}_p$ generated by the class $a = \bar{X}$ of X in K.
(3) In other words, $K = \mathbb{F}_p[a]$ where a is a root of u.
(4) The isomorphism class of K is independent of the choice of u.

Proof of Lemma 1.3 (5). We prove the following more general result

Lemma 2.1. *Let K be a field. Let G be a finite subgroup of $K^\times$ (=multiplicative group of K). Then G is cyclic.*

Proof. We first prove the lemma when $|G| = \ell^k$ for some prime number ℓ. In such a case Euler-Lagrange theorem implies that any element g of G has an order ℓ^s for some $s \in \mathbb{N}$, $s \leq k$. Let $g_0 \in G$ be an element which has the largest order m. Then we see that any element of G satisfies the equation

$$x^m = 1.$$

Since K is a field, there is at most m solutions to the equation. Thus $|G| \leq m$. So we conclude that the order m of g_0 is equal to $|G|$ and that G is generated by g_0.

Let us proceed now to the general case. Let us factorize the order $|G|$:

$$|G| = \ell_1^{k_1}\ell_2^{k_2}\dots\ell_t^{k_t} \qquad (\ell_1,\ell_2,\dots,\ell_t : \text{prime},\ k_1,k_2,\dots,k_t \in \mathbb{Z}_{>0}).$$

Then G may be decomposed into product of p-subgroups

$$G = G_1 \times G_2 \times \dots \times G_t \qquad (|G_j| = \ell_j^{k_j} (j = 1,2,3,\dots,t)).$$

By using the first step of this proof we see that each G_j is cyclic. Thus we conclude that G is also a cyclic group. □

Exercise 2.1. Let G be a finite abelian group. Assume we have a decomposition $|G| = m_1 m_2$ of the order of G such that m_1 and m_2 are coprime. Then show the following:

(1) Let us put
$$H_j = \{g \in G; g^{m_j} = e_G\} \qquad (j = 1,2)$$
Then H_1, H_2 are subgroups of G.
(2) $|H_j| = m_j$ $(j = 1,2)$.
(3) We have
$$G = H_1 H_2.$$

Exercise 2.2. Let G_1, G_2 be finite cyclic groups. Assume $|G_1|$ and $|G_2|$ are coprime. Show that $G_1 \times G_2$ is also cyclic.

2.1. **Affine schemes.** We define affine schemes as a representable functor.

DEFINITION 2.2. Let R be a ring. Then we denote by $\mathrm{Spec}(R)$ the **affine scheme with coordinate ring** R.

For any affine scheme $\mathrm{Spec}(R)$ and for any ring S, we define the S**-valued point** of $\mathrm{Spec}(R)$ by

$$\mathrm{Spec}(R)(S) = \mathrm{Hom}_{\mathrm{ring}}(R, S)$$

LEMMA 2.3. *Let k be a ring. Let $\{f_1, f_2, \dots, f_m\}$ be a set of equations in n-variables $X_1, X_2, \dots, X_n$ over k. Let us put*

$$A = k[X_1, X_2, \dots, X_n]/(f_1, f_2, \dots, f_m).$$

Then we have a natural identification

$$V(f_1, f_2, \dots, f_m)(K) = \mathrm{Spec}(A)(K)$$

for any algebra K over k.

COROLLARY 2.4. *We employ the assumption as the Lemma. Then:*

(1) *When the "target algebra" K is given, the set of solutions $V(f_1, f_2, \dots, f_m)(K)$ depends only on the affine coordinate ring A.*
(2) *For any element $P \in \mathrm{Spec}(A)(K)$, the "evaluation map"*

$$A \ni f \mapsto \mathrm{eval}_P(f) \in K$$

is defined in an obvious way. Thus every element of A may be regarded as a K-valued function on $\mathrm{Spec}(A)(K)$.

2.2. **localization.**

DEFINITION 2.5. Let f be an element of a commutative ring A. Then we define the localization A_f of A with respect to f as a ring defined by

$$A_f = A[Y]/(Yf - 1)$$

where Y is a indeterminate.

LEMMA 2.6. *When K is a field, then we have a canonical identification*

$$\mathrm{Spec}(A_f)(K) = \{P \in \mathrm{Spec}(A)(K); \mathrm{eval}_P(f) \neq 0\}.$$