Mertens' theorems for Galois extensions

Combinatorial and Additive Number Theory 2016 (Graz)

Seiken Saito (Waseda University)

Jan 6 2016 (16:30-17:00)

Contents

(Main results include a generalization of Williams' theorem.)

This talk is based on my joint work with Takehiro Hasegawa (Shiga Univ.).

Figure: Franz Mertens(1840–1927). From Wikipedia.

Mertens' theorem

Theorem 1 (Mertens theorem (1874))

As $x \to \infty$,

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) = \frac{e^{-\gamma}}{\log x} + O\left(\frac{1}{\log^2 x}\right),$$

where $\gamma = 0.57721\ldots$ *is Euler's constant.*

[Mertens] F. Mertens, Ein Beitrag zur analytischen Zahlentheorie, J. Reine Angew. Math. **78** (1874), 46-62.

The generalization by K.S. Williams

Theorem 1 (Mertens' theorem (1874))

As $x \to \infty$,

$$\prod_{p \le x} \left(1 - \frac{1}{p}\right) = \frac{e^{-\gamma}}{\log x} \left(1 + O\left(\frac{1}{\log x}\right)\right).$$

Theorem 2 (Williams' theorem (1974))

Let q and a be coprime natural numbers. There exists a constant $C(q, a) > 0$ such that, as $x \to \infty$,

$$\prod_{\substack{p \le x \\ p \equiv a \pmod{q}}} \left(1 - \frac{1}{p}\right) = \frac{C(q, a)}{(\log x)^{1/\phi(q)}} \left(1 + O\left(\frac{1}{\log x}\right)\right).$$

Here, $\phi(q)$ is Euler's totient.

The constant $C(q,a)$

Theorem 3 (Williams' theorem (1974))

$$C(q,a) = \left(\frac{q}{\phi(q) \cdot e^{\gamma}} \prod_{\chi \neq \chi_0} \left(\frac{K(1,\chi)}{L(1,\chi)} \right)^{\overline{\chi}(a)} \right)^{1/\phi(q)},$$

where the product of the RHS is taken over all non-trivial Dirichlet characters χ mod q.

$L(s,\chi) = \prod_p \left(1 - \chi(p)p^{-s}\right)^{-1}$ $(\mathrm{Re}(s) > 1)$: the Dirichlet L-function,

$K(s,\chi) := \prod_p \left(1 - k_\chi(p)p^{-s}\right)^{-1}$ $(\mathrm{Re}(s) > 0)$: the K-function, where

$$k_\chi(p) := p\left(1 - \frac{1 - \chi(p)/p}{(1 - 1/p)^{\chi(p)}}\right).$$

[Williams] K. S. Williams, Mertens' Theorem for arithmetic progressions, J. Number Theory **6** (1974), 353-359.

A limit formula for the constant $C(q,a)$

Theorem 4 (Languasco and Zaccagnini (2007))

$$C(q,a)^{\phi(q)} = e^{-\gamma} \lim_{x\to\infty} \prod_{2\le p\le x} \left(1-\frac{1}{p}\right)^{\alpha(p;q,a)},$$

(conditionally convergent). Here,

$$\alpha(p;q,a) := \begin{cases} \phi(q)-1 & (\text{if } p \equiv a \pmod{q}), \\ -1 & (\text{otherwise}). \end{cases}$$

[L-Z] A. Languasco and A. Zaccagnini, A note on Mertens' formula for arithmetic progressions, J. Number Theory **127** (2007), no. 1, 37-46.

$$\prod_{\substack{p \leq x \\ p \equiv a \pmod{q}}} \left(1 - \frac{1}{p}\right) = \frac{C(q,a)}{(\log x)^{1/\phi(q)}} \left(1 + O\left(\frac{1}{\log x}\right)\right),$$

$$C(q,a) = \left(\frac{q}{\phi(q) \cdot e^{\gamma}} \prod_{\chi \neq \chi_0} \left(\frac{K(1,\chi)}{L(1,\chi)}\right)^{\overline{\chi}(a)}\right)^{1/\phi(q)}.$$

By the class field theory,

$$p \equiv a \pmod{q}$$

is equivalent that

$$(\text{the Frobenius automorphism of } p \text{ for } L/\mathbf{Q}) = g$$

for some abelian extension $\exists L/\mathbf{Q}$ and $\exists g \in \mathrm{Gal}(L/\mathbf{Q})$.

Problem

What are the generalization of Williams' and Languasco-Zaccagnini's results for Galois extensions of number fields?

Mertens theorem for a Galois extension of a number field

L/K : a Galois extension with $\mathrm{Gal}(L/K) = G$,

$\mathfrak{O}_K$: the ring of algebraic integers of K,

$\mathfrak{p}$: a prime ideal of K, $\mathbf{N}\mathfrak{p}$: the absolute norm of $\mathfrak{p}$,

$\mathfrak{P}$: a prime ideal of L lying above $\mathfrak{p}$.

$\varphi_{\mathfrak{P}} = \left(\frac{L/K}{\mathfrak{P}}\right)$: the **Frobenius automorphism** of $\mathfrak{P}$ defined as follows:

Let g be the element of G such that, for every $\alpha \in \mathfrak{O}_K$,

$$\alpha^{\mathbf{N}\mathfrak{p}} \equiv \alpha^g \pmod{\mathfrak{P}}$$

holds. Then

$$\varphi_{\mathfrak{P}} = \left(\frac{L/K}{\mathfrak{P}}\right) := g.$$

Since

$$\varphi_{\mathfrak{P}^a} = \left(\frac{L/K}{\mathfrak{P}^a}\right) = aga^{-1}$$

holds for every $a \in G$, the conjugacy class $\{g\}$ is determined by $\mathfrak{p}$.

Mertens theorem for a Galois extension of a number field

Theorem 5 (Hasegawa and S.)

Let L/K be a Galois extension with $\mathrm{Gal}(L/K) = G$. For every prime ideal $\mathfrak{P}$ of L, let $I_{\mathfrak{P}} := \{\sigma \in G : \mathfrak{P}^\sigma = \mathfrak{P},\ \alpha^\sigma \equiv \alpha \pmod{\mathfrak{P}} (\forall \alpha \in \mathfrak{O}_L)\}$ be the inertia group of $\mathfrak{P}$ over $\mathfrak{p}$ ($e_{\mathfrak{p}} := |I_{\mathfrak{P}}|$). Let $r(\mathfrak{p}; g)$ be the positive rational number defined by

$$r(\mathfrak{p}; g) := \frac{|\varphi_{\mathfrak{P}} I_{\mathfrak{P}} \cap \{g\}|}{|\varphi_{\mathfrak{P}} I_{\mathfrak{P}}|} = \frac{|\varphi_{\mathfrak{P}} I_{\mathfrak{P}} \cap \{g\}|}{e_{\mathfrak{p}}}.$$

Then, for every $g \in G$, there exists a constant $C(g) > 0$ such that

$$\prod_{\mathbf{N}\mathfrak{p} \le x} \left(1 - \frac{1}{\mathbf{N}\mathfrak{p}}\right)^{r(\mathfrak{p};g)} = \frac{C(g)}{(\log x)^{|\{g\}|/|G|}} \left(1 + O\left(\frac{1}{\log x}\right)\right), \quad (x \to \infty).$$

Note that, if $\mathfrak{p}$ is unramified in L/K then $I_{\mathfrak{P}} = \{id\}$ and

$$r(\mathfrak{p}; g) = \begin{cases} 1 & (\text{if } \varphi_{\mathfrak{P}} \in \{g\}), \\ 0 & (\text{otherwise}). \end{cases}$$

The constant $C(g)$

Theorem 6 (Hasegawa and S.)

$$C(g) = \left(\frac{1}{\varkappa_K \cdot e^{\gamma}} \prod_{\rho \neq 1_G} \left(\frac{\mathcal{K}(1,\rho)}{\mathcal{L}(1,\rho)} \right)^{\overline{\chi}_\rho(g)} \right)^{|\{g\}|/|G|},$$

where the product of the RHS is taken over all non-trivial irreducible unitary representations ρ of G and χ_ρ is the character of ρ.

$$\mathcal{L}(s,\rho) := \prod_{\mathfrak{p}} \det\left(I - \rho(\varphi_{\mathfrak{P}})(N\mathfrak{p})^{-s}; V^{I_{\mathfrak{P}}}\right)^{-1} \ (\mathrm{Re}(s) > 1) : \text{ the Artin } L,$$

$$\mathcal{K}(s,\rho) := \prod_{\mathfrak{p}} (1 - k_\rho(s,\mathfrak{p}))^{-d_{\rho_{\mathfrak{P}}}^2} \quad (\mathrm{Re}(s) > 1/2) : \text{ ``the } K\text{-function''},$$

$$k_\rho(s,\mathfrak{p}) := 1 - \left(\frac{\det(I - \rho_{\mathfrak{P}}(\varphi_{\mathfrak{P}})(\mathbf{N}\mathfrak{p})^{-s})}{(1 - (\mathbf{N}\mathfrak{p})^{-s})^{\chi_{\rho_{\mathfrak{P}}}(\varphi_{\mathfrak{P}})}} \right)^{1/d_{\rho_{\mathfrak{P}}}^2}, \quad (d_\rho : \text{ the degree of } \rho)$$

$$\varkappa_K := \operatorname*{Res}_{s=1} \zeta_K(s), \quad (\text{the residue of the Dedekind zeta } \zeta_K(s) \text{ at } s = 1).$$

For more information about the formula

$$C(g) = \left(\frac{1}{\varkappa_K \cdot e^{\gamma}} \prod_{\rho \neq 1_G} \left(\frac{\mathcal{K}(1,\rho)}{\mathcal{L}(1,\rho)} \right)^{\overline{\chi}_\rho(g)} \right)^{|\{g\}|/|G|}.$$

Let $\rho_{\mathfrak{P}}$ be the subrepresentation of $\rho : G \to \mathrm{End}(V)$ defined by the restriction V to $V^{I_{\mathfrak{P}}}$:

$$\rho_{\mathfrak{P}} = \rho|_{V^{I_{\mathfrak{P}}}} : \mathbf{C}[G_{\mathfrak{P}}/I_{\mathfrak{P}}] \to \mathrm{End}(V^{I_{\mathfrak{P}}}),$$

which is explicitly given by $\rho_{\mathfrak{P}}(\varphi_{\mathfrak{P}}^m) := \dfrac{1}{e_{\mathfrak{p}}} \sum_{\tau \in I_{\mathfrak{P}}} \rho(\varphi_{\mathfrak{P}}^m \tau)$ for $m \in \mathbf{Z}_{\geq 1}$.

Then $\mathcal{L}(s,\rho)$ and $\mathcal{K}(s,\rho)$ are written as follows:

$$\mathcal{L}(s,\rho) = \exp\left(\mathrm{tr} \sum_{\mathfrak{p}} \sum_{m \geq 1} \frac{1}{m \mathbf{N}\mathfrak{p}^{ms}} \rho_{\mathfrak{P}}(\varphi_{\mathfrak{P}}^m) \right), \quad (\mathrm{Re}(s) > 1),$$

$$\mathcal{K}(s,\rho) = \prod_{\mathfrak{p}} \left(\frac{\det(I - \rho_{\mathfrak{P}}(\varphi_{\mathfrak{P}})(\mathbf{N}\mathfrak{p})^{-s})}{(1 - (\mathbf{N}\mathfrak{p})^{-s})^{\chi_{\rho_{\mathfrak{P}}}(\varphi_{\mathfrak{P}})}} \right)^{-1}, \ (\mathrm{Re}(s) > \frac{1}{2}).$$

A limit formula for the constant $C(g)$

Theorem 7 (Hasegawa and S.)

$$C(g)^{|G|/|\{g\}|} = \frac{1}{\varkappa_K \cdot e^{\gamma}} \lim_{x\to\infty} \prod_{\mathbf{N}\mathfrak{p}\le x} \left(1 - \frac{1}{\mathbf{N}\mathfrak{p}}\right)^{\alpha(\mathfrak{p};g)},$$

(conditionally convergent). Here,

$$\alpha(\mathfrak{p};g) := \frac{|G|}{|\{g\}|} \cdot r(\mathfrak{p};g) - 1.$$

Proof of $\prod_{\mathbf{N}\mathfrak{p}\le x}\left(1-\frac{1}{\mathbf{N}\mathfrak{p}}\right)^{r(\mathfrak{p};g)} = \frac{C(g)}{(\log x)^{|\{g\}|/|G|}}\left(1+O\left(\frac{1}{\log x}\right)\right)$

By the orthogonality of characters:

$$\sum_{\rho\in\widehat{G}} \chi_\rho(h)\overline{\chi}_\rho(g) = \begin{cases} \dfrac{|G|}{|\{g\}|} & \text{if } h\in\{g\}, \\ 0 & \text{otherwise,} \end{cases}$$

we have

$$\sum_{\rho\in\widehat{G}} \chi_{\rho_{\mathfrak{P}}}(\varphi_{\mathfrak{P}})\overline{\chi}_\rho(g) = \frac{1}{e_{\mathfrak{p}}}\sum_{\tau\in I_{\mathfrak{P}}}\sum_{\rho\in\widehat{G}} \chi_\rho(\varphi_{\mathfrak{P}}\tau)\overline{\chi}_\rho(g)$$

$$= \frac{1}{e_{\mathfrak{p}}}\cdot\frac{|G|}{|\{g\}|}\cdot\left|\{\ \tau\in I_{\mathfrak{P}} : \varphi_{\mathfrak{P}}\tau\in\{g\}\ \}\right|$$

$$= \frac{|G|}{|\{g\}|}\cdot\frac{|\varphi_{\mathfrak{P}} I_{\mathfrak{P}}\cap\{g\}|}{e_{\mathfrak{p}}} = \frac{|G|}{|\{g\}|}\cdot r(\mathfrak{p};g).$$

Proof of $\prod_{\mathbf{N}\mathfrak{p}\le x}\left(1-\frac{1}{\mathbf{N}\mathfrak{p}}\right)^{r(\mathfrak{p};g)} = \frac{C(g)}{(\log x)^{|\{g\}|/|G|}}\left(1+O\left(\frac{1}{\log x}\right)\right)$

It follows that

$$\prod_{\mathbf{N}\mathfrak{p}\le x}\left(1-\frac{1}{\mathbf{N}\mathfrak{p}}\right)^{r(\mathfrak{p};g)\cdot|G|/|\{g\}|} = \prod_{\rho\in\widehat{G}}\left(\prod_{\mathbf{N}\mathfrak{p}\le x}\left(1-\frac{1}{\mathbf{N}\mathfrak{p}}\right)^{\chi_{\rho_{\mathfrak{P}}}(\varphi_{\mathfrak{P}})}\right)^{\overline{\chi}_\rho(g)}$$

$$= \prod_{\mathbf{N}\mathfrak{p}\le x}\left(1-\frac{1}{\mathbf{N}\mathfrak{p}}\right)\cdot\prod_{\rho\ne 1_G}\left(\prod_{\mathbf{N}\mathfrak{p}\le x}\left(1-\frac{1}{\mathbf{N}\mathfrak{p}}\right)^{\chi_\rho(\varphi_{\mathfrak{P}})}\right)^{\overline{\chi}_\rho(g)} \qquad (1)$$

Proof of $\displaystyle\prod_{\mathbf{N}\mathfrak{p}\le x}\left(1-\frac{1}{\mathbf{N}\mathfrak{p}}\right)^{r(\mathfrak{p};g)} = \frac{C(g)}{(\log x)^{|\{g\}|/|G|}}\left(1+O\left(\frac{1}{\log x}\right)\right)$

By the definition of $k_\rho(s,\mathfrak{p})$, we have

$$\left(1-\frac{1}{\mathbf{N}\mathfrak{p}}\right)^{\chi_{\rho_{\mathfrak{P}}}(\varphi_{\mathfrak{P}})} = \det\left(I-\rho_{\mathfrak{P}}(\varphi_{\mathfrak{P}})\frac{1}{\mathbf{N}\mathfrak{p}}\right)(1-k_\rho(1,\mathfrak{p}))^{-d^2_{\rho_{\mathfrak{P}}}}.$$

Since $\mathcal{L}(s,\rho)$ and $\mathcal{K}(s,\rho)$ are holomorphic at $s=1$, we obtain

$$\prod_{\mathbf{N}\mathfrak{p}\le x}\det\left(I-\rho(\varphi_{\mathfrak{P}})\frac{1}{\mathbf{N}\mathfrak{p}}\right) = \frac{1}{\mathcal{L}(1,\rho)}+O\left(\frac{1}{\log x}\right), \quad (\text{for } \rho\neq 1_G)$$

$$\prod_{\mathbf{N}\mathfrak{p}\le x}(1-k_\rho(\mathfrak{p}))^{-1} = \mathcal{K}(1,\rho)+O\left(\frac{1}{x}\right), \quad (\text{for } \rho\in\widehat{G}).$$

Thus,

$$\prod_{\rho\neq 1_G}\left(\prod_{\mathbf{N}\mathfrak{p}\le x}\left(1-\frac{1}{\mathbf{N}\mathfrak{p}}\right)^{\chi_\rho(\varphi_{\mathfrak{P}})}\right)^{\overline{\chi}_\rho(g)}$$

$$= \prod_{\rho\neq 1_G}\left(\frac{\mathcal{K}(1,\rho)}{\mathcal{L}(1,\rho)}\right)^{\overline{\chi}_\rho(g)} + O\left(\frac{1}{\log x}\right). \qquad (2)$$

Proof of $\displaystyle\prod_{\mathbf{N}\mathfrak{p}\le x}\left(1-\frac{1}{\mathbf{N}\mathfrak{p}}\right)^{r(\mathfrak{p};g)} = \frac{C(g)}{(\log x)^{|\{g\}|/|G|}}\left(1+O\left(\frac{1}{\log x}\right)\right)$

By the Mertens theorem for the number field K (see [Rosen]),

$$\prod_{\mathbf{N}\mathfrak{p}\le x}\left(1-\frac{1}{\mathbf{N}\mathfrak{p}}\right) = \frac{1}{e^{\gamma}\varkappa_K}\cdot\frac{1}{\log x}\left(1+O\left(\frac{1}{\log x}\right)\right). \qquad (3)$$

Applying (2) and (3) to (1), we have

$$\begin{aligned}&\prod_{\mathbf{N}\mathfrak{p}\le x}\left(1-\frac{1}{\mathbf{N}\mathfrak{p}}\right)^{r(\mathfrak{p};g)\cdot|G|/|\{g\}|}\\ &= \prod_{\mathbf{N}\mathfrak{p}\le x}\left(1-\frac{1}{\mathbf{N}\mathfrak{p}}\right)\prod_{\rho\ne 1_G}\left(\prod_{\mathbf{N}\mathfrak{p}\le x}\left(1-\frac{1}{\mathbf{N}\mathfrak{p}}\right)^{\chi_\rho(\varphi_{\mathfrak{P}})}\right)^{\overline{\chi}_\rho(g)}\\ &= \frac{C(g)^{|G|/|\{g\}|}}{\log x}\left(1+O\left(\frac{1}{\log x}\right)\right). \qquad \square\end{aligned}$$

[Rosen] M. Rosen, A generalization of Mertens' theorem, J. Ramanujan Math. Soc. **14** (1999), no. 1, 1-19.

Proof of $C(g)^{|G|/|\{g\}|} = \dfrac{1}{\varkappa_K \cdot e^\gamma} \lim_{x\to\infty} \prod_{\mathbf{N}\mathfrak{p}\le x} \left(1 - \dfrac{1}{\mathbf{N}\mathfrak{p}}\right)^{\alpha(\mathfrak{p};g)}$

$$\prod_{\mathbf{N}\mathfrak{p}\le x}\left(1-\frac{1}{\mathbf{N}\mathfrak{p}}\right)^{r(\mathfrak{p};g)} = \frac{C(g)}{(\log x)^{|\{g\}|/|G|}}\left(1+O\left(\frac{1}{\log x}\right)\right) \qquad (1)$$

$$\prod_{\mathbf{N}\mathfrak{p}\le x}\left(1-\frac{1}{\mathbf{N}\mathfrak{p}}\right) = \frac{1}{e^\gamma \varkappa_K}\cdot\frac{1}{\log x}\left(1+O\left(\frac{1}{\log x}\right)\right) \qquad (2)$$

By raising (1) to the power $|G|/|\{g\}|$, and dividing by (2), we have

$$\prod_{\substack{\mathbf{N}\mathfrak{p}\le x\\ \varphi_{\mathfrak{P}}\in\{g\}}}\left(1-\frac{1}{\mathbf{N}\mathfrak{p}}\right)^{|G|/|\{g\}|\cdot r(\mathfrak{p};g)} \prod_{\mathbf{N}\mathfrak{p}\le x}\left(1-\frac{1}{\mathbf{N}\mathfrak{p}}\right)^{-1}$$

$$= \varkappa_K\cdot e^\gamma\cdot C(g)^{|G|/|\{g\}|}\left(1+O\left(\frac{1}{\log x}\right)\right).$$

The LHS is equal to $\prod_{\mathbf{N}\mathfrak{p}\le x}(1-1/\mathbf{N}\mathfrak{p})^{\alpha(\mathfrak{p};g)}$. AS $x\to\infty$, we have the assertion. □

Some applications

Theorem 8 (Theorem 3 of [Williams])

Let q and a be coprime natural numbers. As $x \to \infty$,

$$\sum_{\substack{m \leq x \\ p \mid m \Rightarrow p \equiv a \pmod{q}}} \frac{1}{m} \sim \frac{1}{\Gamma\left(1 + \frac{1}{\phi(q)}\right)} \left(\frac{\phi(q)}{q} \prod_{\chi \neq \chi_0} \left(\frac{L(1,\chi)}{K(1,\chi)} \right)^{\overline{\chi}(a)} \right)^{1/\phi(q)} (\log x)^{1/\phi(q)},$$

where the product of the RHS is taken over all non-trivial Dirichlet characters χ mod q.

$L(s,\chi) = \prod_p \left(1 - \chi(p)p^{-s}\right)^{-1}$ $(\mathrm{Re}(s) > 1)$: the Dirichlet L-function,
$K(s,\chi) := \prod_p \left(1 - k_\chi(p)p^{-s}\right)^{-1}$ $(\mathrm{Re}(s) > 0)$: the K-function, where
$k_\chi(p) := p\left(1 - \dfrac{1 - \chi(p)/p}{(1 - 1/p)^{\chi(p)}}\right)$.

Some applications

Theorem 9 (Hasegawa and S.)

Let $L/\mathbf{Q}$ be a Galois extension with $\mathrm{Gal}(L/\mathbf{Q}) = G$, let S be the set of all ramified primes for $L/\mathbf{Q}$, and let $\varphi_p := \varphi_{\mathfrak{P}}$ (where $\mathfrak{P} \subset \mathfrak{O}_L$ is a prime ideal lying above p) be the Frobenius automorphism of p. Then, as $x \to \infty$, we have

$$\sum_{\substack{m \leq x \\ p \mid m \Rightarrow \varphi_p \in \{g\},\ p \notin S}} \frac{1}{m} \sim$$

$$\frac{1}{\Gamma\left(1 + \frac{|\{g\}|}{|G|}\right)} \left(\prod_{\mathfrak{p} \in S} \left(1 - \frac{1}{\mathbf{N}\mathfrak{p}}\right) \prod_{\rho \neq 1_G} \left(\frac{\mathcal{L}_{\mathrm{ur}}(1,\rho)}{\mathcal{K}_{\mathrm{ur}}(1,\rho)} \right)^{\overline{\chi_\rho}(g)} \right)^{\frac{|\{g\}|}{|G|}} (\log x)^{\frac{|\{g\}|}{|G|}}.$$

Here the sum of LHS is taken all positive integers $m \leq x$ such that:

if a prime p divides m then p is unramified for $L/\mathbf{Q}$ and $\varphi_p \in \{g\}$.

That is, every m is a product of unramified primes such that $\varphi_p \in \{g\}$.

Thank you very much for your kind attention!

References

[L-Z] A. Languasco and A. Zaccagnini,
A note on Mertens' formula for arithmetic progressions,
J. Number Theory **127** (2007), no. 1, 37-46.

[Mertens] F. Mertens,
Ein Beitrag zur analytischen Zahlentheorie,
J. Reine Angew. Math. **78** (1874), 46-62.

[Rosen] M. Rosen,
A generalization of Mertens' theorem,
J. Ramanujan Math. Soc. **14** (1999), no. 1, 1-19.

[Williams] K. S. Williams,
Mertens' Theorem for arithmetic progressions,
J. Number Theory **6** (1974), 353-359.