On the History of the *Frobenius*- and *Tchebotarev*-Density

1 Dirichlet Density. Dirichlet (1837)

Definition 1 M a set of prime numbers.

Density $\delta(M)$ of M:

$$\delta(M) := \lim_{s\to 1^+} \sum_{p\in M} \frac{1}{p^s} / \log\frac{1}{s-1}, \qquad s > 1;$$

$$\sum_{p\in M} \frac{1}{p^{1+w}} = \delta(M) log(\frac{1}{w}) + P(w), \quad w > 0,$$

$P(w)$ convergent.

Theorem 2 (Dirichlet 1837)

If $(a, m) = 1$ and

$$M(a) = \{p = mx + a : x \in \mathbb{Z},\ p \text{ prime}\},$$

Then

$$\delta(M(a)) = \frac{1}{\varphi(m)} = \frac{1}{\text{number of classes}}$$

is independent of the class $[a]$ modulo m.

φ: Euler function.

Kronecker (2.2.1880)
(programmatic character)

Dedekind (1877)
(Remark on decomposition

Frobenius (Nov. 1880)

Stickelberger

Dedekind

Frobenius —3.6.1882→ Dedekind

Frobenius ←8.6.1882— **Dedekind** (abstract on the decomposition law in normal extensions and its subfields. Existence of Frobenius aut.)

Published 1896

(Hurwitz: letter to Frobenius on the density theorem)

Published 1894: Zur Theorie der Ideale

(Hilbert 1894: Theory of Galoisian Number Fields. Ramification Theory)

Remarks 3:

(1)**Dirichlet:** Theorem 2 follows from

$L(1,\chi) \neq 0$ for $\chi \neq \chi_0$.

Without this property one has only

$\delta(M(a)) \leq \frac{1}{\varphi(m)}$ in general.

(2) Theorem 2 $\Rightarrow$ $L(1,\chi) \neq 0$ for $\chi \neq \chi_0$.

(3) **Weber:** Theorem 2 follows from the fact that there is a class field K over $\mathbb{Q}$ to the congruence group $(\mathbb{Z}/m\mathbb{Z})^{\times}$, namely

$K = \mathbb{Q}(\zeta_m), \quad \zeta_m = e^{\frac{2\pi i}{m}}$.

(4) **Kronecker:** Theorem 2 follows from the fact that

$\phi_m(x) := \mathrm{Irred}(\zeta_m)$ is of degree $\varphi(m)$.

(5) Eisenstein (1847) densities $\rightarrow$ Minkowski $\rightarrow$ Siegel (1935-37) $\rightarrow$ Tamagawa (numbers).

(6) Theorem 2 was motivated by the Quadratic Reciprocity Law (Legendre, Gauss).

2 Kronecker. Irreducibility

Theorem 4: (Gauss 1801)

For p a prime number,

$\phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$

is irreducible (over $\mathbb{Q}$).

Proofs:

Gauss (1801), Kronecker (1845), Schönemann (1846), Eisenstein (1847), Dedekind (1857, for composite p).

Remark 5: Proof by **Kronecker** (1845) by means of polynomials in the polynomial ring: $\mathbb{Q}(\zeta_p) = \mathbb{Q}[x]/\phi_p(x)$.
Suggested by Kummer (1845).

Theorem 6: (Kronecker 1855, 62, 70, 77)
$K = \mathbb{Q}(\sqrt{-d})$ of discriminant $-d < 0$,
$\mathfrak{o}_f$ order in K of conductor f,
$h = h_f$ class number of $\mathfrak{o}_f$,
$\mathcal{C}_1, \ldots, \mathcal{C}_h$ classes of $\mathfrak{o}_f$,
$j(\mathcal{C}_i)$ singular modulus of the class $\mathcal{C}_i$.

Then:

(1) $j(\mathcal{C}_1), \ldots, j(\mathcal{C}_h)$ are algebraic integers (**class invariants**).

(2) $j(\mathcal{C}_1), \ldots, j(\mathcal{C}_h)$ are the roots of a polynomial $H(x) \in K[x]$ of degree h (over K) (**class equation**).

(3) $H(x)$ is **irreducible** over K, hence the $j(\mathcal{C}_i)$ are all conjugate (over K).

(4) $L = K(j(\mathcal{C}_i))$
is independent of the class $\mathcal{C}_i$.

(5) L/K is **abelian** of degree $[L : K] = h$
(hence solvable over $\mathbb{Q}$).

(6) $\mathrm{Gal}(L/K) \cong \mathrm{Cl}(\mathfrak{o}_f)$ class group of $\mathfrak{o}_f$.

(7) If $\mathfrak{o}_f$ is the principal order in K, i. e. $\mathfrak{o}_f = \mathfrak{o}(K)$, then L/K is unramified (conjecture of Kronecker $\rightarrow$ class field theory of Weber).

(8) L is an associate species to K,
i. e. every ideal in K becomes principal in L.

3 Kronecker Density

Kronecker's Program:

$$\begin{array}{lll} \phi_p(x) \in \mathbb{Q}[x] & \text{irreducible} \searrow & \\ & & F(x) \in K[x] \text{ irreducible?} \\ H(x) \in \mathbb{Q}(\sqrt{-d})[x] & \text{irreducible} \nearrow & \end{array}$$

$$\downarrow$$

Kronecker's Program: Algebraic Theory of Polynomial Rings (1882) $\to$ Hilbert $\to$ Grothendieck.

(1) What are the characteristic properties of irreducible polynomials?

(2) Starting point: Dirichlet's and Kummer's Class Number Formula.

Theorem 7: (Main Theorem)
(Kronecker 1880, dedicated to Kummer)
Let $F(x) \in \mathbb{Z}[x]$,
r: number of irreducible factors of $F(x)$,
ν_p: number of solutions of $F(x) \equiv 0$ modulo p, for a prime p.

Then

$$\sum_p \frac{\nu_p}{p^{1+w}} = r \log\left(\frac{1}{w}\right) + P(w), \quad w > 0;$$

$P(w)$ convergent for small w.

$$\lim_{s\to 1+} \sum_p \frac{\nu_p}{p^s} \Big/ \log\left(\frac{1}{s-1}\right) = r, \quad s > 1.$$

Definition 8: (Kronecker 1880)
Let $F(x) \in \mathbb{Z}[x]$ and $k \in \mathbb{N}$.

(1) M_k = set of primes p for which $F(x) \equiv 0$ modulo p has k solutions modulo p
$= \{p : \ \nu_p = k, \ p \text{ prime}\}$

(2) $D_k := \delta(M_k) = \lim_{s\to 1+} \sum_{p\in M_k} \frac{1}{p^s} / \log\left(\frac{1}{s-1}\right)$

Theorem 9:

Let $F(x) \in \mathbb{Z}[x]$, $n =$ degree of $F(x)$,
$r =$ number of irreducible factors of $F(x)$,
$D_k = \delta(M_k)$, $M_k = \{p : \nu_p = k, p \text{ prime}\}$,
$k \in \mathbb{N}$.

Then

(1) $\sum_{k=1}^{n} kD_k = r$, in particular

(2) $\sum_{k=1}^{n} kD_k = 1 \Leftrightarrow F(x)$ is irreducible.

Remarks 10:

(1) *Kummer, Dedekind:* $F(x) \in \mathbb{Z}[x]$, $F(x)$ irreducible, $F(\alpha) = 0$, $K = \mathbb{Q}(\alpha)$, p prime, $p \nmid [\mathfrak{o}(K) : \mathbb{Z}[\alpha]]$.
Decomposition of p in $K = \mathbb{Q}(\alpha)$ $\longleftrightarrow$
Decomposition of $F(x)$ modulo p.

Hence
$M_k = \{p$ prime: p splits off k prime divisors $\mathfrak{p}$, $\mathfrak{p} \mid p$, of first degree in $K\}$

Hence

D_k depends only on the decomposition law of the primes p with respect to $\mathbb{Q}(\alpha)/\mathbb{Q}$.

(2) *Kronecker:* D_k depends only on the Galois group G of $F(x)$: $G = \mathrm{Gal}(F(x))$, in particular on the **affect** $\mathcal{A} = (\mathcal{S}_n : G)$ or the **order of affect** $a = \mid \mathcal{A} \mid = \frac{|\mathcal{S}_n|}{|G|} = \frac{n!}{g}$ of G.

(3) *Kronecker:* The densities D_k exist, if $G = \mathrm{Gal}(F(x)) = \mathcal{S}_n$

Hilbert (1897): If $n-1$ among the n densities D_k exist, then all n densities exist.

Frobenius (1896): The densities D_k exist.

(4) *Kronecker* gives a series of remarkable properties for D_k (without proofs) $\rightarrow$ *Frobenius* (1887) on double congruences $\rightarrow$ on group theory.

Theorem 11:

(1) $F(x) \in \mathbb{Z}[x]$ irreducible, of degree n and galois $\Rightarrow$
$D_i = 0 \quad \text{for } i = 1, \ldots, n-1, \quad D_n = \frac{1}{n}.$

(2) $F(x) \in \mathbb{Z}[x]$ irreducible, of degree $n \Rightarrow$
$D_n = \frac{1}{a} = \frac{g}{n!},$
where $g = |G|, \ G = \mathrm{Gal}(F(x)).$

(3) $F(x) \in \mathbb{Z}[x]$ irreducible $\Rightarrow$ there are infinitely many primes p such that
$F(x) \equiv (x - a_1) \cdots x - a_n)$ modulo p, $a_i \in \mathbb{Z}$.

(4) $F(x) \in \mathbb{Z}[x]$ irreducible,
$F(\alpha) = 0, \quad K = \mathbb{Q}(\alpha) \quad \Rightarrow$ there are infinitely many primes p such that p is completely split in $K = \mathbb{Q}(\alpha)$.

(5) $F(x), \ F'(x) \in \mathbb{Z}[x]$,
$\deg F(x) = \deg F'(x) = q$ prime.
$\nu_p = \nu'_p$ for all $p \quad \Rightarrow \quad D_i = D'_i$
for all $i = 1, \ldots, q \quad \Rightarrow \quad N = N'$,
where N, N' are the normal fields of F and F'.

Remarks 12:

(1) *Kronecker*: (5) is a Local-Global-Principle (Boundary Problem for all primes).

(2) For $F(x)$ *abelian,* this boundary problem is solved by Class Field Theory (Decomposition Law).

Theorem 13:

Let α be a primitive λ-th root of unity,
$F(x) = x^{\lambda-1} + x^{\lambda-2} + \ldots + x + 1$, λ prime,
$F(\alpha) = 0$, $G(x) = \text{Irred}\,(\alpha)$, $r = \deg G(x)$.

$$\begin{aligned} M_1 &= \{p = \lambda x + 1 : x \in \mathbb{Z},\ p \text{ prime}\} \\ &= \{p \text{ prime: } F(x) \equiv 0 \text{ modulo } p \text{ admits } \lambda - 1 \text{ roots}\} \end{aligned}$$

Then

(1) $\delta(M_1) = \frac{1}{r}$

(2) $r = \lambda - 1$,

hence $F(x) = G(x)$, and $F(x)$ is irreducible.

Proof: From the Class Number Formula

(Kronecker gives only a sketch $\to$ Weber)

$$\lim_{s\to 1^+} \log \frac{\prod_{\chi\neq\chi_0} L(s,\chi)}{s-1} = \lim_{s\to 1^+} \sum_{p\in M_1} \frac{\lambda-1}{p^s}$$

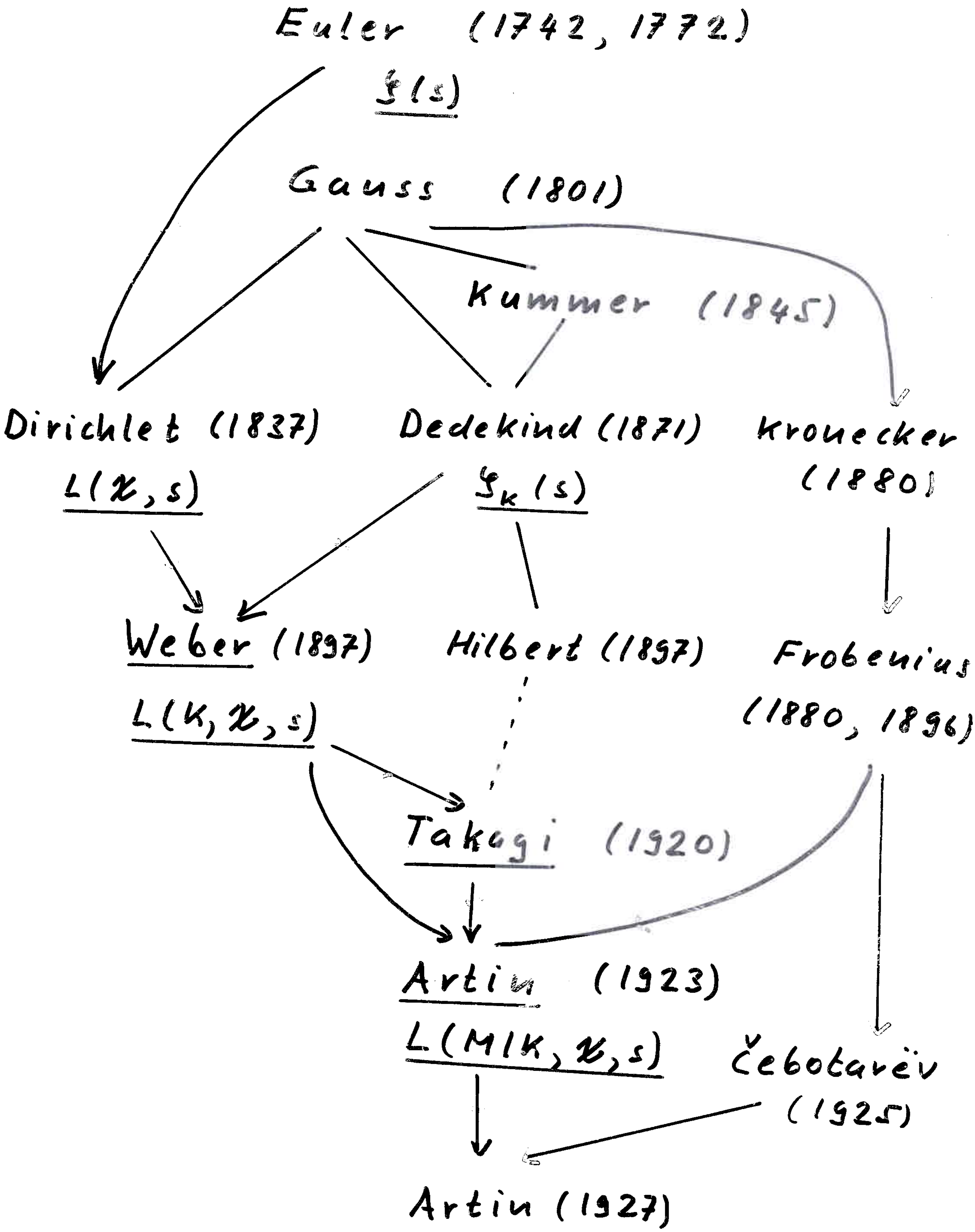
$$= \frac{\lambda-1}{r} \log \frac{1}{s-1}.$$

Remarks 14:

(1) *Kronecker:* Key point
Regulator $\neq 0 \;\Rightarrow\; L(1,\chi)\neq 0$ for $\chi\neq\chi_0$.

(2) Can be generalized to λ composite.

(3) Analogous proof for the Class Equation
$H(x)\in K[x],\quad K=\mathbb{Q}(\sqrt{-d})$.
M_1 is replaced by
$M = \{p$ prime: $(\frac{-d}{p}) = 1$, p is represented by the principal class of binary quadratic forms of discriminant $-d\}$.



Euler (1742, 1772)
$\zeta(s)$
Gauss (1801)
Kummer (1845)
Dirichlet (1837)
$L(\chi, s)$
Dedekind (1871)
$\zeta_K(s)$
Kronecker (1880)
Weber (1897)
$L(K, \chi, s)$
Hilbert (1897)
Frobenius (1880, 1896)
Takagi (1920)
Artin (1923)
$L(M|K, \chi, s)$
Čebotarëv (1925)
Artin (1927)

4 Frobenius and Tchebotarev Density

Theorem 15: (Frobenius 1896)

$N/\mathbb{Q}$ normal of degree $h = [N : \mathbb{Q}]$ and discriminant $d(N/\mathbb{Q})$, $\quad H = \mathrm{Gal}(N/\mathbb{Q})$,
$\mathfrak{o} = \mathfrak{o}(N)$ integers in N.
For any prime ideal $\mathfrak{p} \subseteq \mathfrak{o}$ with $\mathfrak{p} \not| \, d(N/\mathbb{Q})$, there exists a unique *substitution*

$$\sigma = F = F_{\mathfrak{p}} \in H \quad \text{such that}$$

$$F(\omega) \equiv \omega^p \quad \text{modulo } \mathfrak{p}, \quad \text{for all } \omega \in \mathfrak{o},$$

where $\mathfrak{p} \mid p$, i. e. $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$.

Theorem 16:

Let $\mathfrak{p} \subseteq \mathfrak{o}$, $\mathfrak{p}$ a prime ideal in N, $\mathfrak{p} \not| \, d(N/\mathbb{Q})$, $H = \mathrm{Gal}(N/\mathbb{Q})$.
Then

(1) $F_{\mathfrak{p}^\sigma} = \sigma^{-1} F_{\mathfrak{p}} \sigma, \quad \sigma \in H.$

(2) $p \mapsto [F_{\mathfrak{p}}] = \{\sigma^{-1} F_{\mathfrak{p}} \sigma : \sigma \in H\} = F(p)$

is well defined and depends only on p.

Problem:

Given $\tau \in H = \mathrm{Gal}(N/\mathbb{Q})$,
$C = [\tau] = \{\sigma^{-1}\tau\sigma : \sigma \in H\}$,
the conjugacy class of τ,
$M_C = \{p \text{ primes: } F(p) = C\}$,
determine $D_C := \delta(M_C)$.

Theorem 17: (Frobenius 1896)
Let $N/\mathbb{Q}$ be normal, $H = \mathrm{Gal}(N/\mathbb{Q})$,
$C_1, C_2, \dots, C_l$ the conjugacy classes in H,
$h_\lambda = |C_\lambda|$, $\lambda = 1, 2, \dots, l$.

$\mathfrak{p}$ a prime ideal in N, $\mathfrak{p} \nmid d(N/\mathbb{Q})$, $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$,
$F = F_\mathfrak{p}$ the Frobenius substitution of $\mathfrak{p}$, $F \in C_\lambda$,
$v_\lambda = |\{\sigma \in H : \sigma^{-1}F\sigma = F\}|$.
$h = |H| = h_\lambda v_\lambda$, $\lambda = 1, 2, \dots, l$.

$M_\lambda = \{p \text{ primes: } F(p) = C_\lambda\}$.

If $H = \mathcal{S}_n$, then

$$\sum_{p \in M_\lambda} \frac{1}{p^{1+w}} = \frac{h_\lambda}{h} \log\left(\frac{1}{w}\right) + P_\lambda(w), \quad \text{i. e.}$$

$$D_\lambda = \delta(M_\lambda) = \frac{h_\lambda}{h} = \frac{1}{v_\lambda}.$$

Remark:

For general $H = \mathrm{Gal}(N/\mathbb{Q})$, Frobenius could only show a weaker result:

Theorem 18:

$N/\mathbb{Q}$ normal, $H = \mathrm{Gal}(N/\mathbb{Q})$, $h = |H|$.
$F \in F(p)$, $f = | < F > |$ the order of F,

$\mathcal{A}(F) = \bigcup_{(r,f)=1} F(p)^r = \bigcup_{(r,f)=1} [F^r]$

the **division** of F,

$\mathcal{A}_1, \ldots, \mathcal{A}_l$ all divisions in H,

$a_\lambda = |\{\sigma \in H : \sigma \in \mathcal{A}_\lambda\}| = |\mathcal{A}_\lambda|$

the number of substitutions lying in $\mathcal{A}_\lambda$,

$A_\lambda = \{p \text{ primes: } F(p) \subseteq \mathcal{A}_\lambda\}$.

Then

$$\delta(A_\lambda) = \frac{a_\lambda}{h}.$$

Theorem 19: (Tchebotarev, 1925)

Theorem 17 is true for any Galois group $H = \mathrm{Gal}(N/\mathbb{Q})$ over $\mathbb{Q}$. .

Remark 20:

Theorem 19 was already conjectured by Frobenius (1896).