Chebotarëv and his Density Theorem[1]

P. Stevenhagen and H. W. Lenstra, Jr.

Introduction

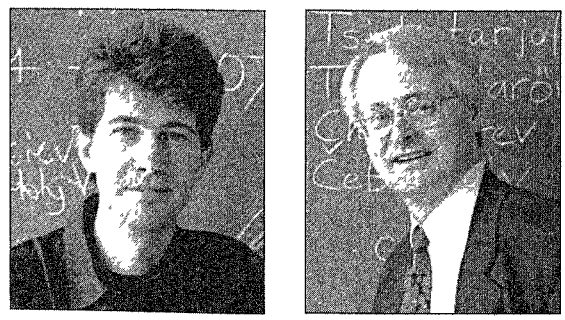
The fame of the Russian number-theorist Nikolaĭ Grigor'evich Chebotarëv[2] (1894–1947) rests almost exclusively on his proof, in 1922, of a conjecture of Frobenius, nowadays known as *Chebotarëv's density theorem.* Algebraic-number-theorists have cherished the theorem ever since, because of both its beauty and its importance.

In the present article we introduce Chebotarëv and his theorem. Drawing upon Russian sources, we describe his life and the circumstances under which he proved his density theorem. Two characteristic examples are given to illustrate the nature of his other work. Next we explain the content of his theorem, reducing to a minimum the specialized terminology in which the theorem is usually couched. We shall see that the key idea of Chebotarëv's proof enabled Artin to prove his reciprocity law; in fact, had history taken a slightly different course, then Chebotarëv would have proven it first. For the connoisseur, we give, in an appendix, a paraphrase of Chebotarëv's proof of his density theorem. It uses no class field theory, and it is appreciably more elementary than the treatment found in current textbooks.

We shall not discuss the important role that Chebotarëv's density theorem plays in modern arithmetic algebraic geometry. The interested reader is referred to [34] and [35].

Life

Nikolaĭ Grigor'evich Chebotarëv was born in Kamenets-Podolsk on June 15, 1894; on June 3 according to the Julian calendar that was still in use in Russia. His father, Grigoriĭ Nikolaevich, served in the Russian court system in several Ukrainian cities and was president of a district court when the 1917 revolution interrupted his career. It left him stripped of his status and reduced to poverty, and he died of cholera in Odessa in 1922. Nikolaĭ had one younger brother, Grigoriĭ, a doctor who was seen in the White Army during the civil



P. Stevenhagen and H. W. Lenstra, Jr.

The Dutch mathematicians *P. Stevenhagen* (Universiteit van Amsterdam) and *H. W. Lenstra, Jr.* (University of California, Berkeley) count algebra and number theory among their interests and the history of mathematics among their hobbies.

They organized the Density celebration on June 15, 1994, at the Universiteit van Amsterdam. This event commemorated the centenary of Chebotarëv. The present article is based on two lectures that were delivered on that occasion.

P. Stevenhagen received doctoral degrees both from the University of California at Berkeley and from the Universiteit van Amsterdam.

H. W. Lenstra, Jr. has a degree from the Universiteit van Amsterdam and an honorary degree from the Université de Franche-Comté in Besançon. He is a member of the Koninklijke Nederlandse Akademie van Wetenschappen.

[1]The first author thanks I. R. Shafarevich and A. G. Sergeev for providing biographical material on Chebotarev. The second author was supported by NSF under grant No. DMS 92-24205. Part of the work reported in this article was done while the second author was on appointment as a Miller Research Professor in the Miller Institute for Basic Research in Science. D. J. Bernstein, J. A. Buchmann, G. H. Frei, A. C. P. Gee, S J. P. Hillion, A. Schinzel, and V. M. Tikhomirov kindly provided assistance.

[2]The transliteration of Cyrillic names in this paper follows the current *Mathematical Reviews* standard.

war following the revolution. He emigrated to Yugoslavia and never returned to the Soviet Union.

Nikolaĭ received an upper-class education that was strictly controlled by his mother. It is no coincidence that mathematics, a domain beyond her control, became Nikolaĭ's favorite pastime when he was 15 or 16 years old. He was often unable to attend school during this time, as he suffered from pleurisy, and in the winter of 1910–1911 he was taken by his mother to the Italian Riviera to recover from pneumonia. In 1912 he gained admission as a student in mathematics to the university in Kiev, then known as the University of the Holy Vladimir. He was a student of D. A. Grave, as were B. N. Delonè, who later tried unsuccessfully to lure Chebotarëv to Leningrad, and Otto Shmidt, who would become a renowned group-theorist as well as vice president of the Academy of Sciences. Grave was a former student of Chebyshev and Korkin, and at that time the only true mathematician in Kiev. In these years, Nikolaĭ's mathematical interests took shape. Despite the difficulties arising from World War I, which necessitated the temporary relocation of the university to Saratov, he graduated in 1916 and became Privatdozent after his magister's exam in 1918. He continued to live like a student, earning money from private lessons and teaching in high schools. In 1921 he moved to Odessa to assist his parents, who were subsisting there under miserable conditions. After his father's death, his mother eked out a living by selling cabbage at the market.

Despite professional and economic support from local mathematicians such as Shatunovskiĭ and Kagan, Nikolaĭ had difficulties finding a suitable position in Odessa: the mathematics there was focused primarily on foundational issues, and these were alien to Nikolaĭ's interests.

Then came the summer of 1922. Chebotarëv recalls the circumstances in a 1945 letter to M. I. Rokotovskiĭ [8], who had tried to interest him in his plans for a thesis on the working environment of scientists:

> In real life, scientists come in as many varieties as there are species of plants. You describe a tender rose, that needs a supporting stake, fertilized soil, regular watering, and so on, in order to grow. Our harsh reality would more likely yield thistles, which produce somewhat crude but beautiful flowers under all conditions. What would our science be like, if our scientists could only work in silence or with "good, not too loud music" in their offices? I belong to the older generation of Soviet scientists, who were shaped by the circumstances of a civil war. I devised my best result while carrying water from the lower part of town (Peresypi in Odessa) to the higher part, or buckets of cabbages to the market, which my mother sold to feed the entire family.

This "best result" was *Chebotarëv's density theorem*. It was a spark from heaven, which would secure Chebotarëv a comfortable position in Soviet mathematics and immortalize his name in algebraic number theory.

The difficult financial situation of the Chebotarëv household improved considerably in 1923, when Nikolaĭ married the teacher and assistant physiologist Mariya Alexandrovna Smirnitskaya. Working with a former student of the famous physiologist Pavlov, she made a decent salary. The relationship with her mother-in-law, who had insisted in vain on a religious marriage, seems to have been less than friendly.

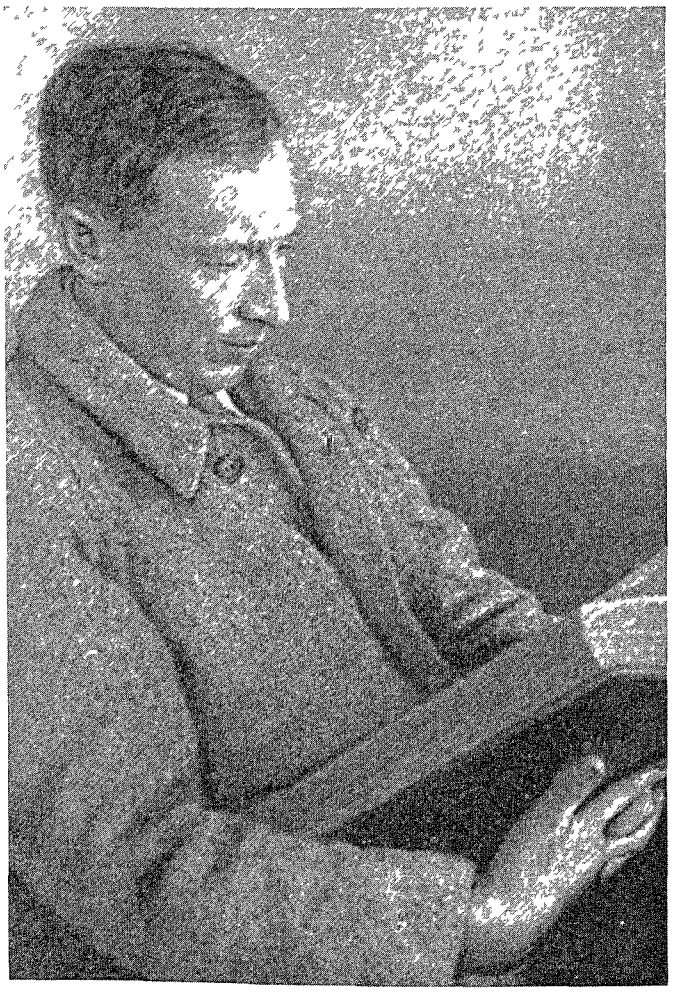
In 1924, Nikolaĭ finally found a job at the Civil Engineering Institute in Moscow. Here he became acquainted with the Kazan mathematician N. N. Parfent'ev—his first tie to Kazan. Nikolaĭ was icily received by his Moscow colleagues; he found out that he occupied D. F. Egorov's position, and resigned after 7 months. Egorov, who had shaped the Moscow school of pure mathematics together with his student N. N. Luzin, had been dismissed for political reasons. Eventually, he would be arrested as a "religious sectarian" and go on a hunger strike. Mortally ill, he would be transported to a prison hospital in Kazan in 1931, where Nikolaĭ's wife happened to work as a doctor [36]. He is purported to have died at the Chebotarëv home.

Back in Odessa, Nikolaĭ got a badly paid and ill-defined position as secretary for scientific research at an Educational Institute. His situation did not become more comfortable in 1926, when his son, named Grigoriĭ in accordance with family tradition, was born. Scientifically, however, he did very well. A talented 17-year-old boy, Mark Kreĭn, who had come to Odessa, started working under Nikolaĭ's supervision and assembled enough students for a seminar on algebraic

functions. When Nikolaĭ left Odessa in 1927, Kreĭn continued the seminar and founded a school in functional analysis. Before this, in 1925, Nikolaĭ had been able to make his first scientific trip abroad, to the meeting of the German Mathematical Society (DMV) in Danzig, where he met E. Noether, Hensel, and Hensel's student Hasse. He traveled on to Berlin, visiting I. Schur, and to Gottingen, where he met his countryman A. M. Ostrovskiĭ. Like Nikolaĭ, Ostrovskiĭ was a student of Grave from Kiev. Grave had sent him abroad to continue his education, as Jews could not attend graduate schools in tsarist Russia. Nikolaĭ greatly impressed Ostrovskiĭ by providing an original solution to one of Ostrovskiĭ's problems. We will discuss it later in this section.

In 1927, Nikolaĭ finally defended his doctoral dissertation, which was based on his 1922 density theorem, at the Ukrainian Academy of Sciences. He had earlier been invited by Delonè to do so in Leningrad, but this was no longer possible: the bourgeois custom of the doctoral degree had been abolished in the Russian republic in 1926. Shortly after receiving his doctorate, Nikolaĭ was offered positions both in Leningrad, which already had a strong group of algebraists, and in the provincial town of Kazan, some 800 kilometers east of Moscow, where he would have to create his own school. At that time, the university of Kazan boasted its own journal, in which Nikolaĭ had already published a few papers, and a rich library. It had an international reputation because it regularly awarded a prestigious prize in geometry named after Lobachevskiĭ, the famous geometer who had worked in Kazan during the 19th century. Unfortunately, the independence of the provincial universities was gradually suppressed during the Stalin era, and by 1945 both the journal and the prize were abolished, as were most scientific contacts with capitalist countries. After some hesitation, Nikolaĭ finally chose Kazan, where he was to stay for the rest of his life. He left Odessa in December 1927. His wife and son followed in the spring of 1928. This put an end to the difficulties of sharing accommodations with Nikolaĭ's mother, who went to live with her sisters in Krasnodar. She died in 1939.

In Kazan, Nikolaĭ was able to create his own school of algebra, and his students obtained positions in several Soviet universities. During his Kazan period, his work gained ample recognition in the Soviet Union. He was elected corresponding member of the Academy of Sciences in 1929 and invited to speak at the All-Union congress in Leningrad in 1934. In 1943, he became Honored Scientist of the Russian republic. He was nominated for the Stalin Prize in 1943 and 1946, but received this coveted prize only posthumously, in 1948. It was awarded for his work on Hilbert's thirteenth problem concerning the impossibility of solving the 7th-degree equation by means of continuous functions of two arguments. In 1954 it turned out that one of his results on this problem was incorrect, a counterexample being due to his own son Grigoriĭ, who had also become a mathematician [22].



N. G. Chebotarëv

Chebotarev's reputation did not remain confined to the Soviet Union. In 1932, he accepted the invitation to deliver a plenary address at the international congress in Zurich. His talk, "Problems in contemporary Galois theory" ([7], vol. 3, pp. 5–46) marked the 100th anniversary of the death of Galois.

Nikolaĭ remained productive during the 20 years he spent in Kazan. The research papers in his collected works [7] address a wide range of problems—many in number theory and in his "official" specialty, Galois theory, but others in Lie groups, abelian integrals, the distribution of zeros of polynomials, and approximation theory. Apart from this, he produced course notes in advanced algebra, the calculus of variations, and topology. His textbook *Osnovy teorii Galua* (*Basic Galois theory*) appeared in two volumes in 1934 and 1937, together with a 1936 monograph *Teoriya Galua* that included results on the inverse problem and the theory of resolvents. A reedited and extended German translation of the first volume with inclusions from the monograph appeared

in 1950, after a 10-year delay caused by the war [9]. Nikolaĭ's interest in resolvents led him to study Lie groups. The result was his *Teoriya grupp Li*, the first Russian textbook on Lie groups, which appeared in 1940. It was followed by a posthumously published monograph *Teoriya algebraicheskikh funktsiĭ*. In addition, Nikolaĭ devoted a lot of energy to editing the collected works of Zolotarëv. He initiated the publication of the collected works of Galois in Russian in 1936, whose translation was carried out by his favorite student N. N. Meĭman. Other projects of his, such as the creation of an encyclopedia of elementary mathematics, were to remain unfinished when, during the spring of 1947, Nikolaĭ started suffering from a stomach cancer. An operation became inevitable. In June 1947 he was hospitalized in the Sklifosovskiĭ Institute in Moscow. He survived the operation but died from complications 11 days later, on July 2.

The Chebotarëv family played an important role in the academic social life in Kazan. The new spacious house they obtained in 1937 was a meeting place for students, scientific visitors, and other guests. Nikolaĭ had his working place in the house—somewhat surprisingly not a desk but a bed—and an extensive library of reprints consisting largely of the many papers he reviewed for the *Zentralblatt*. During the war, the universities and certain academic institutions of Moscow and besieged Leningrad were moved to Kazan, and flocks of scientists crowded the university there. Housing was problematic. It was not uncommon for the Chebotarëv residence to have as many as 20 overnight guests.

Despite his aversion to administrative duties, Nikolaĭ succeeded Parfent'ev as head of Kazan's department of mathematics and physics in 1943. During the 1930s he had been the director of NIIMM, a scientific institute for mathematics and mechanics at the university. This function caused frequent disputes between Nikolaĭ and the rector of the university. Otherwise, it seems that his easygoing character and his thoughtful politeness usually kept him out of conflict.

We illustrate the style of Chebotarëv's mathematics by presenting two results with which he was particularly pleased. The first is the solution to the problem posed to him by Ostrovskiĭ in Göttingen. It held implications for the number of singularities of certain lacunary complex power series on the boundary of their domain of convergence [32]. Chebotarëv himself calls it ([8], pp. 5–6) "a very modest result," mentioning the compliments the "gloomy and sombre" Ostrovskiĭ made to him on its account, and observing that it "does meet the requirements of mathematical esthetics."

PROBLEM. *Let p be a prime number and $\zeta \in \mathbf{C}$ a primitive pth root of unity. Show that all minors of the Vandermonde determinant $|\zeta^{rs}|_{r,s=0}^{p-1}$ are different from zero.*

Ostrovskiĭ tried in vain to deduce this from known results on determinants and from elementary estimates on absolute values of complex numbers. Chebotarëv's novel idea was to show that such minors, which are clearly elements of $\mathbf{Q}(\zeta)$, the pth cyclotomic field over the field of rational numbers $\mathbf{Q}$, do not vanish in the p-adic completion $\mathbf{Q}_p(\zeta)$ of $\mathbf{Q}(\zeta)$. Just as every p-adic number has a p-adic expansion, so does every element of $\mathbf{Q}_p(\zeta)$ have a π-adic expansion for $\pi = \zeta - 1$. Thus, each of the determinant entries can be expanded as

$$\zeta^{rs} = (1+\pi)^{rs} = 1 + \binom{rs}{1}\pi + \binom{rs}{2}\pi^2 + \cdots .$$

Using the linearity of determinants with respect to their columns, we can expand a minor of size $n \times n$ correspondingly as

$$M = |\zeta^{r_i s_j}|_{i,j=1}^{n} = \left|\sum_{k\geq 0}\binom{r_i s_j}{k}\pi^k\right|_{i,j=1}^{n} = \sum_{k_1,\ldots,k_n}\begin{vmatrix}\binom{r_1 s_1}{k_1} & \cdots & \binom{r_1 s_n}{k_n}\\ \vdots & & \vdots\\ \binom{r_n s_1}{k_1} & \cdots & \binom{r_n s_n}{k_n}\end{vmatrix}\pi^{k_1+\cdots+k_n}.$$

Write $D_{k_1,\ldots,k_n}$ for the determinants occurring in the right-hand side. If, for some $d < n$, there are at least $d+1$ values in the sequence $k_1, k_2, \ldots, k_n$ that are smaller than d, then $D_{k_1,\ldots,k_n}$ vanishes, for the entries of its jth column are the values in the r_i's of the polynomial $\binom{s_j X}{k_j}$ of degree k_j, and $d+1$ polynomials of degree smaller than d are linearly dependent. It follows that $D_{k_1,\ldots,k_n}$ vanishes for $k_1 + k_2 + \cdots + k_n < 0 + 1 + \cdots + (n-1) = n(n-1)/2$, and that in the case of equality $k_1 + k_2 + \cdots + k_n = n(n-1)/2$, it can only be nonzero if the sets $\{k_1, k_2, \ldots, k_n\}$ and $\{0, 1, \ldots, n-1\}$ coincide. In that case, $D_{k_1,\ldots,k_n}$ is a Vandermonde determinant. We find $M = C\pi^{n(n-1)/2} + O(\pi^{1+n(n-1)/2})$, where the constant C is given by

$$C = \sum_{\sigma} \operatorname{sign}(\sigma)\,\frac{s_1^{\sigma(0)}\, s_2^{\sigma(1)} \cdots s_n^{\sigma(n-1)}}{0!\,1!\,2!\cdots(n-1)!}\prod_{1\leq i<j\leq n}(r_j - r_i).$$

Here σ ranges over the permutations of $\{0, 1, \ldots, n-1\}$. We recognize once more a Vandermonde determinant, obtaining

$$C = \frac{\prod_{1\leq i<j\leq n}(r_j - r_i)\prod_{1\leq i<j\leq n}(s_j - s_i)}{0!\,1!\,2!\cdots(n-1)!}.$$

As C is an integer coprime to p, it is not divisible by π, and we find that M has π-adic valuation $n(n-1)/2$. Note that this valuation depends only on the *size* of M. In particular, M is nonzero. This finishes the proof.

The problem has a large number of published solutions: A. Danilevskiĭ (1937), Yu. G. Reshetnyak (1955), and M. Newman (1975) adapted Chebotarëv's proof in

various ways, Dieudonné reproved the theorem independently in 1970 (see [13])

The second problem we discuss is of a very classical nature Chebotarev took it up as a suitable example to be included in his textbook on Galois theory As with the previous problem and the density theorem, he managed to "dig deeper" with existing tools and find what others had failed to uncover We start with an observation that goes back to Hippocrates of Chios (~430 B C) Let ABC be an isosceles right-angled triangle as in Figure 1 Then the area of the shaded *lune* that is bounded by the arcs on AB of the circumscribed circle of ABC and the circle tangent to AC and BC is equal to the area of the triangle ABC The discovery that it was possible to square certain lunes caused some excitement in antiquity, as it is clearly a promising step toward the solution of the famous problem of *squaring the circle*

More generally, let m and n be positive integers, with $m > n$ Consider a lune that is bounded by two arcs on AB such that the angles $\angle AMB$ and $\angle ANB$ at their respective centers M and N have ratio m n, thus, in Figure 2, where $m = 3$ and $n = 2$, we have 2μ $2\nu = 3$ 2 Draw m equal chords in the outer arc and n equal chords in the inner arc, as in Fig 2 the chords AC, CD, and DB have equal lengths, as have the chords AE and EB The $m + n$ angles subtended by these chords at the centers of the corresponding arcs are then all equal, so the $m + n$ circle segments cut out by these chords are all similar It follows that the ratio of the area of an outer segment and the area of an inner segment equals the square of the ratio of the radii of the two arcs Suppose now that this square happens to be n m Then the total area of the m outer segments equals the total area of the n inner segments, in Fig 2, the area of the three segments on AC, CD, and DB equals the area of the segments on AE and EB Therefore, the area of the lune equals the area of the "rectified" lune, i e , the polygonal area (like $AEBDC$ in Fig 2) that is bounded by the $m + n$ chords Note that this area is nothing but the area of the tetragon $ANBM$, as the total area of the m triangles with vertex M on the outer chords equals the total area of the n triangles with vertex N on the inner chords In this case we say that the lune can be *squared*

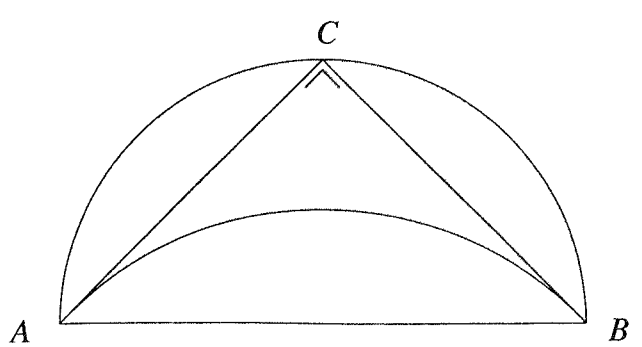


Figure 1

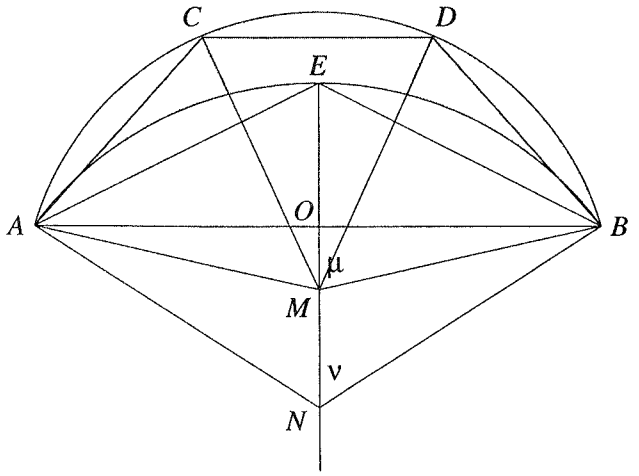


Figure 2

If O is the midpoint of the interval AB and OB has unit length, the radii MB and NB are the inverses of sin μ and sin ν, so if we set $\mu = m\vartheta$ and $\nu = n\vartheta$, the corresponding lune can be squared if and only if the identity

$$\left(\frac{\sin m\vartheta}{\sin n\vartheta}\right)^2 = \frac{m}{n} \tag{$*$}$$

holds This is an algebraic equation in $x = \cos\vartheta$, and if it has a root that is *constructible*, we find an example of a squarable lune that can be constructed It clearly depends only on the *ratio* m n whether the corresponding lune can be squared The problem of the quadrature of lunes can be formulated as follows

PROBLEM. *Find all ratios* m n *of coprime positive integers for which the equation* $(*)$ *has a constructible solution* $x = \cos\vartheta$

The example in Figure 1 corresponds to the case m $n = 2$ 1, which yields $x = 1/\sqrt{2}$ For the ratio m $n = 3$ 2 in Fig 2, already known to Hippocrates, equation $(*)$ is quadratic in $\cos\vartheta$ and the corresponding lune is constructible The constructible lune corresponding to the ratio m $n = 3$ 1 also goes back to Hippocrates, and Clausen [10] published the further examples m $n = 5$ 1 and 5 3 in 1840, not knowing that two of his "four new lunar areas" had already been known to Hippocrates, and the two others to the 18th-century mathematician Martin Johan Wallenius (see [19], p 200) Clausen concludes his paper with the conjecture that there are no further examples

> Ich glaube schwerlich, daß sich die Großen, die die Winkel der andern Verhaltnissen entsprechenden Ausschnitte bestimmen, geometrisch finden lassen
>
> [I find it hard to believe that the quantities that determine the angles of the segments corresponding to other ratios can be found geometrically]

Partial results toward Clausen's conjecture were obtained by Landau (1903) and the Bulgarian mathematician Chakalov (1929–1930), who wrote equation (4) in terms of a new variable $y = e^{2i\theta}$ as

$$F(y) = (y^m - 1)^2 - \frac{m}{n} y^{m-n}(y^n - 1)^2 = 0$$

and determined in a few cases the Galois groups of the irreducible factors of F over $\mathbf{Q}$. Note that F is a difference of squares in $\mathbf{Q}(\sqrt{m/n})$ in the easier case where $m - n$ is *even*. By a careful study of the *arithmetical* properties of the polynomial F, in particular the ramification of the splitting field of F over $\mathbf{Q}$, Chebotarev showed in 1934 that Clausen's list is complete in this easier case [6]. The general case remained open, but shortly before Chebotarev's untimely death in 1947, his student A. B. Dorodnov finished the work of his teacher and proved Clausen's conjecture in full [15].

The Density Theorem

Chebotarev's density theorem may be regarded as the least common generalization of Dirichlet's theorem on primes in arithmetic progressions (1837) and a theorem of Frobenius (1880, published 1896).

Dirichlet's theorem is easy to discover experimentally. Here are the prime numbers below 100, arranged by final digit:

1	11, 31, 41, 61, 71
2	2
3	3, 13, 23, 43, 53, 73, 83
5	5
7	7, 17, 37, 47, 67, 97
9	19, 29, 59, 79, 89

It does not come as a surprise that no prime numbers end in 0, 4, 6, or 8, and that only two prime numbers end in 2 or 5. The table suggests that there are infinitely many primes ending in each of 1, 3, 7, 9, and that, approximately, they keep up with each other. This is indeed true, it is the special case $m = 10$ of the following theorem, proved by Dirichlet (1805–1859) in 1837 (see [14]). Write $\varphi(m)$ for the number of integers x with $1 \le x \le m$ and $\gcd(x, m) = 1$, so $\varphi(10) = 4$.

THEOREM OF DIRICHLET. *Let m be a positive integer. Then for each integer a with $\gcd(a, m) = 1$ the set of prime numbers p with $p \equiv a \bmod m$ has density $1/\varphi(m)$.*

Here we say that a set S of prime numbers has *density* δ if

$$\left(\sum_{p \in S} \frac{1}{p^s}\right)\left(\sum_{p \text{ prime}} \frac{1}{p^s}\right)^{-1} \to \delta \quad \text{for } s \downarrow 1$$

Clearly, the set of all prime numbers has density 1. Finite sets of prime numbers have density 0, since $\sum_{p \text{ prime}} 1/p$ diverges. Thus, for $m = 10$, the "exceptional" primes 2 and 5 do not count from a density point of view, and the other primes are "equidistributed" over the four residue classes 1, 3, 7, 9 modulo 10 in the sense that the four densities are equal. Dirichlet's original formulation of his theorem does not involve the notion of density, but the above is what his proof gives.

The notion of density that we just defined is sometimes called *analytic* or *Dirichlet* density. It would have been more intuitive to say that a set S of prime numbers has density δ if

$$\frac{\#\{p \le x \;\; p \in S\}}{\#\{p \le x \;\; p \text{ prime}\}} \to \delta \quad \text{for } x \to \infty$$

With this concept of density, called *natural* density, Dirichlet's theorem is also valid, but the proof, which is much harder, was only given by De la Vallée-Poussin in 1896 (see [11]). If a set of primes has a natural density, then it has an analytic one, and the two densities are equal, but the converse is false. The results below were originally proved for the analytic density, which is easier to manipulate. They are also valid for the natural density, but in this case the proofs require additional techniques, largely due to Hecke [20].

The theorem of Frobenius (1849–1917) that Chebotarev generalized deserves to be better known than it is. For many applications of Chebotarev's theorem it suffices to have Frobenius's theorem, which is both older (1880) and easier to prove than Chebotarev's theorem (1922).

Again, Frobenius's theorem can be discovered empirically. Consider a polynomial f with integer coefficients, say $f = X^4 + 3X^2 + 7X + 4$, and suppose that one is interested in deciding whether or not f is irreducible over the ring $\mathbf{Z}$ of integers. A standard approach is to factor f modulo several prime numbers p. Thus, we have

$$f \equiv X(X^3 + X + 1) \mod 2,$$

where X and $X^3 + X + 1$ are irreducible over the field $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z}$ of 2 elements. We say that the *decomposition type* of f modulo 2 is 1, 3. It follows that *if* f is reducible over $\mathbf{Z}$, then its decomposition type will likewise be 1, 3 a product of a linear factor and an irreducible cubic factor. However, the latter alternative is incompatible with the fact that the decomposition type modulo 11 is 2, 2:

$$f \equiv (X^2 + 5X - 1)(X^2 - 5X - 4) \mod 11,$$

where the two factors are irreducible over $\mathbf{F}_{11}$. One concludes that f is irreducible over $\mathbf{Z}$.

Could the irreducibility of f have been proven with a *single* prime? Modulo such a prime number, f would

have to be irreducible, with decomposition type equal to the single number 4 Current computer algebra packages make it easy to do a numerical experiment There are 168 prime numbers below 1000 Two of these, $p = 7$ and $p = 19$, are special, in the sense that f acquires repeated factors modulo p

$$f \equiv (X - 3)^2(X + 3)^2 \mod 7,$$
$$f \equiv (X - 3)^3(X + 9) \mod 19$$

For no other prime does this happen, and the following types are found

Type 1, 3	112 primes (67 5%),
Type 2, 2	44 primes (26 5%),
Type 1, 1, 1, 1	10 primes (6 0%)

It is suggested that the primes with type 1, 3 have density ^{2}, that the primes with type 2, 2 have density , that no prime at all exists with the desired type 4 or with type 1, 1, 2, and, to make the densities add up to 1, that the primes with type 1, 1, 1, 1 have density $_{2}$

The following table shows the results of similar experiments performed on several fourth-degree polynomials For each polynomial f in the first column, the table gives the apparent density of primes p for which f modulo p has a given decomposition type

f	4	1,3	2,2	1,1,2	1,1,1,1
$X^4 - X - 1$	$_{4}$		$_{8}$	$_{4}$	$_{24}$
$X^4 - X^2 + 1$	0	0	$_{3}$ $_{4}$	0	$_{1}$
$X^4 + X^3 + X^2 + X + 1$	$_{2}$	0	$_{4}$	0	$_{1}$ $_{4}$
$X^4 - X^2 - 1$	$_{4}$	0	$_{8}$		$_{8}$
$X^4 + 3X^2 + 7X + 4$	0	^{2}	$_{4}$	0	$_{2}$

Frobenius's theorem tells how to understand these fractions through the *Galois group* of the polynomial

Let, generally, f be a polynomial with integer coefficients and with leading coefficient 1, and denote the degree of f by n Assume that the discriminant $\Delta(f)$ of f does not vanish, so that f has n distinct zeros $\alpha_1, \alpha_2, \ldots, \alpha_n$ in a suitable extension field of the field $\mathbf{Q}$ of rational numbers Write K for the field generated by these zeros $K = \mathbf{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ The Galois group G of f is the group of field automorphisms of K Each $\sigma \in G$ permutes the zeros $\alpha_1, \alpha_2, \ldots, \alpha_n$ of f, and is completely determined by the way in which it permutes these zeros Hence, we may consider G as a subgroup of the group S_n of permutations of n symbols Writing an element $\sigma \in G$ as a product of disjoint cycles (including cycles of length 1), and looking at the lengths of these cycles, we obtain the *cycle pattern* of σ, which is a partition $n_1, n_2, \ldots, n_t$ of n

If p is a prime number not dividing $\Delta(f)$, then we can write f modulo p as a product of distinct irreducible factors over $\mathbf{F}_p$ The degrees of these irreducible factors form the decomposition type of f modulo p, this is also a partition of n Frobenius's theorem asserts, roughly speaking, that the "number" of primes with a given decomposition type is proportional to the number of $\sigma \in G$ with the same cycle pattern

THEOREM OF FROBENIUS. *The density of the set of primes p for which f has a given decomposition type $n_1, n_2, \ldots, n_t$ exists, and it is equal to $1/\#G$ times the number of $\sigma \in G$ with cycle pattern $n_1, n_2, \ldots, n_t$*

Consider, for example, the partition in which all n_i are equal to 1 Only the identity permutation has this cycle pattern Hence, the set of primes p for which f modulo p splits completely into linear factors has density $1/\#G$ Thus, the last column of the table above indicates that the Galois groups of the five polynomials in the table have orders 24, 4, 4, 8, and 12, respectively In fact, these Galois groups are the full symmetric group S_4, the Klein four group V_4, the cyclic group C_4, the dihedral group D_4 of order 8, and the alternating group A_4 This is a complete list of transitive subgroups of S_4, so that every irreducible f of degree 4 behaves like one of the five polynomials in the table For reducible f there are other possibilities

The alternating group A_4 contains, in addition to the identity element, eight elements of type 1, 3, and three elements of type 2, 2 This explains the fractions $_{12}^{8} = {}^{2}_{3}$ and $_{12} =$ that we found for the polynomial $f = X^4 + 3X^2 + 7X + 4$ Since A_4 contains no elements of type 4, the set of primes p for which f is irreducible modulo p has density zero In fact, the existence of the Frobenius substitution (see below) implies that no such primes exist at all

With a little group theory, one can deduce several charming consequences from Frobenius's theorem For example, if f modulo p has a zero in $\mathbf{F}_p$ for every prime number p, then f is either linear or reducible Also, the number of irreducible factors of f over $\mathbf{Z}$ is equal to the average number of zeros of f modulo p in $\mathbf{F}_p$, averaged over all p (in an obvious way) Historically, the logic went in the opposite direction the last statement was proved by Kronecker in 1880 [23], and it formed the basis for Frobenius's proof, it was Frobenius who used group theory in his argument, not Kronecker

In order to see a connection between the theorems of Dirichlet and Frobenius we consider polynomials of the type $f = X^m - 1$, where m is a positive integer We have $\Delta(X^m - 1) = (-1)^{m(m-1)/2}m^m$, so we exclude the primes dividing m For the remaining primes p, one can determine the decomposition type of $X^m - 1$ modulo p by applying elementary properties of finite fields (see [25], Theorem 2 47) With $m = 12$ one finds in this way that the decomposition type depends only on the residue class of p modulo 12, as follows

$p \equiv 1 \mod 12$	1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1
$p \equiv 5 \mod 12$	1, 1, 1, 1, 2, 2, 2, 2
$p \equiv 7 \mod 12$	1, 1, 1, 1, 1, 1, 2, 2, 2
$p \equiv 11 \mod 12$	1, 1, 2, 2, 2, 2, 2

Notice that the four decomposition types corresponding to the four coprime residue classes are pairwise distinct Hence, Frobenius's theorem implies the special case $m = 12$ of Dirichlet's theorem This does not work for all m For example, with $m = 10$ we find in the same way the following decomposition types

$p \equiv 1 \bmod 10$	1, 1, 1, 1, 1, 1, 1, 1, 1, 1
$p \equiv 3$ or $7 \bmod 10$	1, 1, 4, 4
$p \equiv 9 \bmod 10$	1, 1, 2, 2, 2, 2

The decomposition type depends only on p modulo 10, but Frobenius's theorem does not distinguish between the residue classes 3 mod 10 and 7 mod 10 Generally, Frobenius's theorem for $f = X^m - 1$ is implied by Dirichlet's theorem for the same m, but not conversely

One can formulate a sharper version of Frobenius's theorem that for $f = X^m - 1$ does come down to Dirichlet's theorem To do this, one needs to answer a question that is suggested by the connection between decomposition types and cycle patterns Namely, is it possible to associate in some natural manner, with each prime number p not dividing $\Delta(f)$, an element $\sigma_p \in G$ such that the decomposition type of f modulo p is the same as the cycle type of σ_p? The answer is almost affirmative it can indeed be done, except that σ_p, traditionally called the *Frobenius substitution* of p, is only well defined up to conjugacy in G (Conjugate permutations have the same cycle pattern, so this should not bother us too much) Once the Frobenius substitution has been defined, one can wonder about the density of the set of primes p for which σ_p is equal to a given element of G This leads to the desired common generalization of the theorems of Dirichlet and Frobenius It was formulated as a conjecture by Frobenius, and ultimately proved by Chebotarev

The construction of the Frobenius substitution is mildly technical, which forms the main cause for the relative unpopularity of Chebotarev's theorem outside algebraic number theory In our exposition we shall take a few easily stated facts for granted

First, let a prime number p be fixed, and denote by $\bar{\mathbf{F}}_p$ an algebraic closure of the field $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ The fundamental tool in the theory of finite fields is the *Frobenius map* Frob $\bar{\mathbf{F}}_p \to \bar{\mathbf{F}}_p$, which is defined by $\mathrm{Frob}(\alpha) = \alpha^p$ It clearly respects multiplication, and it respects, miraculously, addition as well it is a *field automorphism* of $\bar{\mathbf{F}}_p$ It follows that Frob permutes the zeros of any polynomial g that has coefficients in $\mathbf{F}_p$ Galois theory for finite fields comes down to the statement that *the cycle pattern* of Frob, *viewed as a permutation of the zeros of* g, *is the same as the decomposition type of* g *over* $\mathbf{F}_p$ This is true for any polynomial g with coefficients in $\mathbf{F}_p$ that has no repeated factors The proof readily reduces to the case that g is irreducible, in which case one applies Theorem 2 14 of [25] The case of interest to us is $g = (f \bmod p)$, with f as taken earlier

The Frobenius map is an automorphism of the field $\bar{\mathbf{F}}_p$ of characteristic p, and the Frobenius substitution σ_p is going to be an automorphism of the field K of characteristic zero To relate the two fields, we develop a way of taking elements of $K = \mathbf{Q}(\alpha_1, \quad , \alpha_n)$ modulo p, so that the "zeros of $(f \bmod p)$" can be regarded as the "(zeros of f) mod p"

By a *place* of K over p we mean a map $\psi: K \to \bar{\mathbf{F}}_p \cup \{\infty\}$ for which

(i) $\psi^{-1}\bar{\mathbf{F}}_p$ is a subring of K, and $\psi\ \psi^{-1}\bar{\mathbf{F}}_p \to \bar{\mathbf{F}}_p$ is a ring homomorphism,
(ii) $\psi x = \infty$ if and only if $\psi(x^{-1}) = 0$, for any nonzero $x \in K$

Note that a new symbol like ∞ is forced upon us if we attempt to take elements of K modulo p we obviously want p mod p to be 0, which leads to $(1/p) \bmod p = 1/0 = \infty$

The basic facts about places are as follows

(a) a place of K over p exists, for any prime number p,
(b) if ψ, ψ' are two places over p, then $\psi' = \psi \circ \tau$ for some $\tau \in G$,
(c) if p does not divide $\Delta(f)$, then the element $\tau \in G$ in (b) is uniquely determined by ψ and ψ'

In the formulation we have chosen, these facts are hard to find in the textbooks This provides an attractive exercise for the reader who is not willing to take them for granted

Let p be any prime number not dividing $\Delta(f)$, and let ψ be a place of K over p It is easily seen that $\psi(\alpha_1)$, $\psi(\alpha_2)$, , $\psi(\alpha_n)$ are the zeros of $(f \bmod p)$ in $\bar{\mathbf{F}}_p$ Applying (b) and (c) to $\psi' = \mathrm{Frob} \circ \psi$ — which is also a place over p, with $\mathrm{Frob}(\infty) = \infty$ — one finds that there is a unique element $\mathrm{Frob}_\psi \in G$ for which

$$\psi \circ \mathrm{Frob}_\psi = \mathrm{Frob} \circ \psi$$

This is going to be our Frobenius substitution As an element of G, it is characterized by

$$\psi(\mathrm{Frob}_\psi(x)) = \mathrm{Frob}(\psi(x)) \quad \text{for all } x \in K$$

This shows that Frob_ψ permutes $\alpha_1, \alpha_2, \quad , \alpha_n$ in the same way as Frob permutes the zeros $\psi(\alpha_1), \psi(\alpha_2), \quad , \psi(\alpha_n)$ of $(f \bmod p)$ Therefore, the cycle pattern of Frob_ψ is indeed equal to the decomposition type of f modulo p

The Frobenius substitution Frob_ψ does, in general, depend on the choice of the place ψ over p By (b), any other place over p is of the form $\psi \circ \tau$, and one readily verifies from the definition that $\mathrm{Frob}_{\psi\circ\tau} = \tau^{-1} \circ \mathrm{Frob}_\psi \circ \tau$, that is, if ψ varies over the places over a fixed prime p, then Frob_ψ ranges over a conjugacy class in G We shall denote a typical element of this conjugacy class by σ_p,

it is well defined only up to conjugacy, and it is called the *Frobenius substitution* of p

To illustrate the above, we consider again the polynomial $f = X^m - 1$ In this case K is a *cyclotomic* field, obtained by adjoining a primitive mth root of unity ζ to $\mathbf{Q}$. The Galois group G has order $\varphi(m)$, and it is naturally isomorphic to the group $(\mathbf{Z}/m\mathbf{Z})^*$ of units of the ring $\mathbf{Z}/m\mathbf{Z}$, here $\tau \in G$ corresponds to $(a \bmod m) \in (\mathbf{Z}/m\mathbf{Z})^*$ if $\tau(\zeta) = \zeta^a$ Let p be a prime number not dividing m Since the Galois group is abelian, the Frobenius substitution σ_p is a well-defined element of G, not just up to conjugacy To compute it, let ψ be a place over p Then $\eta = \psi(\zeta)$ is a primitive mth root of unity in $\mathbf{F}_p$ By definition of σ_p, we have $\psi(\sigma_p(x)) = \psi(x)^p$ for all $x \in K$ Putting $x = \zeta$, and letting a be such that $\sigma_p(\zeta) = \zeta^a$, we find that $\eta^a = \eta^p$, so that $a \equiv p \bmod m$ In other words, *if p is a prime number not dividing m, then the Frobenius substitution σ_p is the element of G that under the isomorphism $G \cong (\mathbf{Z}/m\mathbf{Z})^*$ corresponds to $(p \bmod m)$*

The example just given allows us to reformulate Dirichlet's theorem as follows *if $f = X^m - 1$ for some positive integer m, then the set of prime numbers p for which σ_p is equal to a given element of G has a density, and this density equals* $1/\#G$, thus the Frobenius substitution is equidistributed over the Galois group if p varies over all primes not dividing m Chebotarev's theorem extends this to all f

CHEBOTARËV'S DENSITY THEOREM. *Let f be a polynomial with integer coefficients and with leading coefficient* 1 *Assume that the discriminant $\Delta(f)$ of f does not vanish Let C be a conjugacy class of the Galois group G of f Then the set of primes p not dividing $\Delta(f)$ for which σ_p belongs to C has a density, and this density equals $\#C/\#G$*

On first inspection, one might feel that Chebotarev's theorem is not much stronger than Frobenius's version In fact, applying the latter to a well-chosen polynomial (with the same splitting field as f), one finds a variant of the density theorem in which C is required to be a *division* of G rather than a conjugacy class, here two elements of G belong to the same division if the cyclic subgroups that they generate are conjugate in G Frobenius himself reformulated his theorem already in this way The partition of G into divisions is, in general, less fine than its partition into conjugacy classes, and Frobenius's theorem is correspondingly weaker than Chebotarev's For example, (3 mod 10) and (7 mod 10) belong to the same division of the group $(\mathbf{Z}/10\mathbf{Z})^*$, and this is why Frobenius's theorem cannot distinguish between primes lying in these two residue classes

We close this section with three typical elementary applications of Chebotarev's density theorem For the proofs, it suffices to apply the theorem to appropriately constructed fields, just as one obtains Dirichlet's theorem by looking at cyclotomic fields

The first is a result from algebraic number theory the prime ideals of the ring of integers of an algebraic number field are equidistributed over the ideal classes The proof requires the notion of a *Hilbert class field*

The second has to do with quadratic forms the set of primes p that can be written as $p = 3x^2 + xy + 4y^2$, with $x, y \in \mathbf{Z}$, has a density, which equals $\frac{1}{3}$ Results of this sort depend on *ring class fields*

The final one concerns base 10, like the result with which we started the density of the set of primes p for which $\frac{1}{7}$, when developed in the decimal system, has an odd period length, exists, and is equal to $\frac{1}{2}$ (see [31]) This example depends, interestingly enough, on infinitely many polynomials, namely, those of the form $f = X^{2^k} - 100$ for all $k \geq 2$

Class Field Theory and Chebotarëv's Theorem

The paper in which Frobenius proved his theorem and formulated the conjecture that was to become Chebotarev's density theorem had already been written in 1880 He communicated the results of his paper to Stickelberger and Dedekind, but delayed the publication until Dedekind's ideal theory had appeared in print This occurred in 1894, and Frobenius's paper came out in 1896

Frobenius's conjecture was 42 years old when Chebotarev proved it in 1922 During these 42 years, algebraic number theory had gone through several developments Dedekind and Kronecker laid the foundations of the theory, Hilbert wrote his *Zahlbericht*, Weber and Hilbert conceived the principal theorems of *class field theory*, and shortly after World War I, the Japanese mathematician Takagi supplied the proofs of these theorems (see [18])

Class field theory describes all abelian extensions of a given algebraic number field It is, after more than 70 years, still considered to be a difficult theory Its main results are natural enough, but the proofs are long and winding, they have the character of a verification rather than offering a satisfactory explanation of *why* the results are true

One might think that class field theory provided Chebotarev with a powerful tool for his proof Indeed, modern textbook treatments of Chebotarev's density theorem invariably depend on class field theory (see, for example, [24], Chap VIII, Sec 4 and [30], Chap V, Sec 6) Remarkably, the original proof did not In fact, Chebotarev was at the time not yet familiar with class field theory, he proved his theorem essentially with his bare hands As we shall see, his proof was more important for class field theory than class field theory was for his proof

Chebotarev's argument was based on a new technique of his own invention, which consisted of "crossing" arbitrary abelian extensions of number fields with *cyclotomic* extensions, obtained by adjoining a root of unity Using no more than basic Galois theory,

Chebotarev showed that this procedure reduced the general case of his theorem to the case of (relative) cyclotomic extensions He handled this case by way of a fairly standard argument similar to the one Dirichlet had used More details can be found in Schreier's lucid contemporary account [33] and in the appendix to this article

Chebotarev published his density theorem first in Russian in 1923 [4], and next in German in 1925 [5] Also in 1923, Emil Artin published his reciprocity law [1, Satz 2] This law is now considered to be *the* main result of class field theory, even though it is missing from Weber's and Hilbert's original conception Artin boldly formulated his law as a theorem, but he admitted that he had no proof He pointed out that his reciprocity law would imply Frobenius's conjecture [1, Abschnitt 7] On February 10, 1925, Artin wrote to Hasse [16, p 23]

> Haben Sie die Arbeit von Tschebotareff in den *Annalen* Bd 95 gelesen? Ich konnte sie nicht verstehen und mich auch aus Zeitmangel noch nicht richtig dahinterklemmen Wenn die richtig ist, hat man sicher die allgemeinen Abelschen Reziprozitatsgesetze in der Tasche Das Studium der Arbeit haben wir hier auf das nachste Semester verschoben Vielleicht haben Sie sie schon gelesen und wissen also ob falsch oder richtig?
>
> [Did you read Chebotarev's paper in the *Annalen*, vol 95? I could not understand it, and lack of time prevented me so far from properly concentrating on it If it is correct, then one surely has the general abelian reciprocity laws in one s pocket Here we postponed studying the paper until the next semester Perhaps you have read it already and know therefore whether it is right or wrong?]

Artin's intuition was correct Chebotarev himself writes [7, Vol 3, pp 155–156]

> In the summer of 1927, when I studied class field theory, I became convinced that it was possible to prove Artin's reciprocity law by means of my device of taking composites with cyclotomic extensions When the outline of a proof began to dawn on me, albeit still rather dimly, we returned from the dacha to the city [Odessa], and there I saw in the display case of the library the issue of the *Hamburger Abhandlungen* with Artin s paper [2] My annoyance was immediately mitigated when I saw that Artin mentions at the beginning of his paper that a basic idea of his proof, that of taking composites with cyclotomic extensions, was bor rowed from my paper [5] I was very touched by Artin's meticulousness in matters of attribution, as there is only an incomplete analogy between the ways in which the method of taking composites with cyclotomic extensions is used in the two papers

Artin found his proof in July 1927 (see [16], pp 31–32) Chebotarev was not far behind

Chebotarev's technique is still a crucial ingredient of all known proofs of Artin's reciprocity law (e g , [24], Chap X, Sec 2) It is widely felt that it works for no good reason, and that it is just as counterintuitive as most proofs in class field theory To this complaint, Chebotarev's ghost might reply that it is our intuition and human psychology that need to be replaced, and not his perfectly valid and effective argument Indeed, Neukirch [30] weaves Chebotarev's stratagem so closely through his presentation of the theory that one can believe that one day it will be part of our way of thinking about the reciprocity law

On the other hand, Chebotarev's trick has disappeared from current treatments of his density theorem once the reciprocity law is available, one can deal directly with abelian extensions, without the detour through cyclotomic extensions The reader of the appendix will agree that this approach, due to Deuring [12], is a very natural one, but it makes Chebotarev's theorem appear harder than it actually is

Appendix

We give a proof of Chebotarev's theorem that follows his original strategy, if not his tactics References are to [24] We assume familiarity with basic algebraic number theory, including elementary properties of zeta functions [VIII 1–3], but not including class field theory

We prove a more general version of the theorem, in which the base field can be any algebraic number field F instead of just $\mathbf{Q}$. As in the case $F = \mathbf{Q}$, a set of primes of F can have a *density* [VIII 4] Let K be a finite Galois extension of F, with Galois group G There is again, for all but finitely many primes $\mathfrak{p}$ of F, a *Frobenius substitution* $\sigma_\mathfrak{p}$, which is an element of G that is well defined up to conjugacy

CHEBOTARÈV'S THEOREM. *For any conjugacy class C of G, the density $d(K/F,C)$ of the set of primes $\mathfrak{p}$ of F for which $\sigma_\mathfrak{p} \in C$ exists and equals $\#C/\#G$*

The proof begins with a reduction to the abelian case Let $\sigma \in C$, and put $E = \{x \in K \mid \sigma x = x\}$ Then K is a Galois extension of E with group $\langle\sigma\rangle$ A simple counting argument, carried out in [VIII 4, proof of Theorem 10], shows that

(*) the conclusion of the theorem holds for K, F, C if and only if it holds for $K, E, \{\sigma\}$

Note that the Galois group $\langle\sigma\rangle$ of K over E is abelian

Next one considers the case that K is cyclotomic over F, i e , $K = F(\zeta)$ for some root of unity ζ This is the case that for $F = \mathbf{Q}$ yields Dirichlet's theorem, and it is the proof of the latter theorem that one imitates Using the fact that the Frobenius substitution of a prime $\mathfrak{p}$ depends only on the norm of $\mathfrak{p}$ modulo the order of ζ (cf [VII 4, Example]), one expresses the zeta function $\zeta_K(s)$ of K as a suitable product of L-functions of F Then one looks at the order of the pole in $s = 1$, and one finishes the proof with a traditional argument as in [VIII 4, Corollary to Theorem 8]

One approach to deal with general abelian extensions is by showing that they share the essential properties of cyclotomic extensions that are used This is not easy—it is the content of class field theory It leads to Deuring's proof of Chebotarev's theorem [VIII 4, Theorem 10]

Chebotarev's method does not need class field theory It is as follows Let K be abelian over F, with group G and degree n Let m be any prime number not dividing the discriminant Δ of K over $\mathbf{Q}$, and denote by ζ a primitive mth root of unity Then the Galois group H of $F(\zeta)$ over F is isomorphic to $(\mathbf{Z}/m\mathbf{Z})^*$, and the Galois group of $K(\zeta)$ over F may be identified with $G \times H$ If a prime $\mathfrak{p}$ of F has Frobenius substitution (σ, τ) in $G \times H$, then it has Frobenius substitution σ in G Hence, writing $d_{\inf}$ for *lower* density — defined as the density, but with lim replaced by lim inf — we have $d_{\inf}(K/F, \{\sigma\}) \geq \sum_{\tau \in H} d_{\inf}(K(\zeta)/F, \{(\sigma, \tau)\})$ Now fix $\sigma \in G$ and $\tau \in H$, and suppose that n divides the order of τ Then the subgroups $\langle(\sigma, \tau)\rangle$ and $G \times \{1\}$ of $G \times H$ have a trivial intersection Therefore the field L of invariants of $\langle(\sigma, \tau)\rangle$ satisfies $L(\zeta) = K(\zeta)$, so that the extension $L \subset K(\zeta)$ is cyclotomic By what we proved in the cyclotomic case, the density $d(K(\zeta)/L, \{(\sigma, \tau)\})$ exists and has the correct value This is, by (*), then also true for $d(K(\zeta)/F, \{(\sigma, \tau)\})$, which consequently equals $1/(\#G\ \#H)$ Summing over τ, one obtains $d_{\inf}(K/F, \{\sigma\}) \geq \#H_n/(\#G\ \#H)$, where H_n is the set of $\tau \in H$ of order divisible by n Now it is easy to see that as m ranges over all prime numbers not dividing Δ, the fraction $\#H_n/\#H$ gets arbitrarily close to 1 (use, for example, Dirichlet's theorem to choose $m \equiv 1 \bmod n^k$ for large k) Thus it follows that $d_{\inf}(K/F, \{\sigma\}) \geq 1/\#G$ Applying this to all *other* elements of the group, one finds that the upper density $d_{\sup}(K/F, \{\sigma\})$ is at most $1/\#G$ Therefore the lower and the upper density coincide, and the density equals $1/\#G$ This completes the proof of the theorem

References

Sources on the Life and Work of Chebotarëv The mathematical work of Chebotarev is well documented in books and papers that appeared during or shortly after his lifetime Russian versions of his published papers can be found in his collected works [7] In addition, Chebotarev wrote several overviews of his own mathematical work in volumes appearing under titles of the form *Soviet mathematics after n years*, see, e g , [26] Of a similar nature are [21] and the detailed description of the work of Chebotarev and his students in Kazan by his colleague and friend Morozov [28]

The situation with respect to Chebotarev's life is different His collected works contain a "slightly abridged" version of a mathematical autobiography written in 1927 It focuses on his mathematics and his scientific career, as does, to a lesser extent, the obituary in the *Uspekhi* [29] Morozov wrote a biographical sketch of Chebotarev [27] of a much more personal nature in 1963, when a certain political thaw had set in under Stalin's successor Khrushchev He tried twice without success to publish it in *Algebra i Logika*, on the occasion of the 20th and 25th anniversaries of Chebotarev's death Like Chebotarev's son Grigorii's recollections of his father's life [3] and some selected manuscripts of Chebotarev and Morozov [8], it has not yet been published However, I R Shafarevich has been so kind as to provide us with copies of these documents The amount of detail concerning events of a remotely political nature varies as a function of time in these sources, one can compare the descriptions of similar events in the "abridged" autobiography in the 1949–1950 collected works, in Morozov's 1963 sketch that includes quotes from the unabridged autobiography, and in the recent recollections [3]

1 E Artin, Uber eine neue Art von L-Reihen, Abh Math Sem Univ Hamburg 3 (1923), 89–108, Collected papers, pp 105–124 Addison-Wesley, Reading, MA, 1965
2 E Artin, Beweis des allgemeinen Reziprozitatsgesetzes, Abh Math Sem Univ Hamburg 5 (1927), 353–363, Collected papers, pp 131–141 Addison-Wesley, Reading, MA, 1965
3 G N Chebotarev, *Iz vospominanii ob ottse (From the recollections on my father)* (unpublished)
4 N G Chebotarev, Opredelenie plotnosti sovokupnosti prostykh chisel, prinadlezhashchikh zadannomu klassu podstanovok (Determination of the density of the set of prime numbers, belonging to a given substitution class), Izv Ross Akad Nauk 17 (1923), 205–250, Sobranye sochinenii I, 27–65
5 N Tschebotareff (= N G Chebotarev), Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehoren, Math Ann 95 (1925), 191–228
6 N Tschebotarow (= N G Chebotarev), Uber quadrierbare Kreisbogenzweiecke, I, Math Z 39 (1935), 161–175
7 N G Chebotarev, *Sobranye sochinenii (Collected works)*, Akademiya Nauk SSSR, Moscow, 1949–1950 (3 volumes)
8 N G Chebotarev, Letter to Mikhail Il'ich Rokotovskii, July 3, 1945, in Pis'ma i Vospominaniya (Letters and Recollections) (16 pp , unpublished)
9 N Tschebotarow (= N G Chebotarev), *Grundzuge der Galois schen Theorie*, ubersetzt und bearbeitet von H Schwerdtfeger, Noordhoff, Groningen, 1950
10 Th Clausen, Vier neue mondformige Flachen, deren Inhalt quadrirbar ist, J Reine Angew Math 21 (1840), 375–376
11 Ch de la Vallee-Poussin, Recherches analytiques sur la theorie des nombres premiers Deuxieme partie Les fonctions de Dirichlet et les nombres premiers de la forme lineaire $Mx + N$, Ann Soc Sci Bruxelles 20 (1896), 281–362
12 M Deuring, Uber den Tschebotareffschen Dichtigkeitssatz, Math Ann 110 (1935), 414–415
13 J Dieudonne, Une propriete des racines d'unite, Rev Un Mat Argentina 25 (1970), 1–3, Math Rev 47, #8495, see also [7], Vol 3, p 162, Math Rev 17, 338x, Math Rev 53, #7997
14 G Lejeune Dirichlet, Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthalt, Abh Konigl Akad Wissenschaft Berlin, math Abh (1837), 45–71, Werke I, pp 313–342 Georg Reimer, Berlin, 1889

15 A V Dorodnov, O krugovykh lunochkakh, kvadriruemykh pri pomoshchi tsirkulya i lineĭki (On circular lunes quadrable with the use of ruler and compass), Dokl Akad Nauk SSSR (N S) 58 (1947), 965–968
16 G Frei, *Die Briefe von E Artin an H Hasse* (1923–1953), Collection Mathématique, Département de Mathématiques, Universite Laval, Québec, 1981
17 F G Frobenius, Uber Beziehungen zwischen den Primidealen eines algebraischen Korpers und den Substitutionen seiner Gruppe, Sitzungsberichte Konigl Preußisch Akad Wissenschaft Berlin (1896), 689–703, Gesammelte Abhandlungen II, 719–733 Springer, Berlin, 1968
18 H Hasse, History of class field theory, *Algebraic Number Theory, Proceedings of an Instructional Conference*, (J W S Cassels and A Frohlich, eds), Academic Press, London, 1967, pp 266–279
19 T Heath, *A History of Greek Mathematics*, Oxford University Press, Oxford, 1921, Vol I
20 E Hecke, Uber die L-Funktionen und den Dirichletschen Primzahlsatz fur einen beliebigen Zahlkorper, Nachr Akad Wiss Gottingen Math -Phys Kl (1917), 299–318, Mathematische Werke, 178–197 Vandenhoeck & Ruprecht, Gottingen, 1959
21 *Istoriya otechestvennoĭ matematiki* (*History of our national mathematics*), Naukovo Dumka, Kiev, 1969, vol 3
22 E R Kolchin, Math Rev 17 (1956), 1045
23 L Kronecker, Uber die Irreductibilitat von Gleichungen, Monatsberichte Konigl Preußisch Akad Wissenschaft Berlin (1880), 155–162, Werke II, 83–93 B G Teubner, Leipzig, 1897
24 S Lang, *Algebraic Number Theory*, Addison-Wesley, Reading, MA, 1970
25 R Lidl and H Niederreiter, *Finite Fields*, Addison-Wesley, Reading, MA, 1983
26 *Matematika v SSSR za 30 let, 1917–1947 (Mathematics in the USSR after 30 years, 1917–1947)*, OGIZ, Moscow, 1948
27 V V Morozov, Nikolaĭ Grigor'evich Chebotarev (28 pp , unpublished)
28 V V Morozov, Kazanskaya matematicheskaya shkola za 30 let — algebra (The Kazan mathematical school after 30 years — algebra), Usp Mat Nauk 2(6) (1947), 3–8
29 N G Chebotarev — nekrolog (N G Chebotarev — obituary), Usp Mat Nauk 2(6) (1947), 68–71
30 J Neukirch, *Class Field Theory*, Springer-Verlag, Berlin, 1986
31 R W K Odoni, A conjecture of Krishnamurthy on decimal periods and some allied problems, J Number Theory 13 (1981), 303–319
32 A M Ostrowski, Uber Singularitaten gewisser mit Lucken behafteten Potenzreihen Mathematische Miszellen, VII, Jahresber Deutsch Math -Verein 35 (1926), 269–280, Collected mathematical papers 5, 181–192 Birkhauser, Basel, 1985
33 O Schreier, Uber eine Arbeit von Herrn Tschebotareff, Abh Math Sem Univ Hamburg 5 (1927), 1–6
34 J-P Serre, *Abelian l-Adic Representations and Elliptic Curves*, W A Benjamin, New York, 1969
35 J-P Serre, Quelques applications du théorème de densité de Chebotarev, Publ Math I H E S 54 (1981), 123–201, Œuvres III, 563–641 Springer, Berlin, 1986
36 A L Shields, Luzin and Egorov, Math Intelligencer 9(4) (1987), 24–27

Faculteit Wiskunde en Informatica
Universiteit van Amsterdam
Plantage Muidergracht 24
1018 TV Amsterdam
The Netherlands

Department of Mathematics #3840
University of California
Berkeley, CA 94720-3840, USA

Which Is to Be Master—IV[1]

Chandler Davis

All over the world there are mathematics graduate students who are obliged to start practicing their new science in a new language. They did their undergraduate work in Bulgarian and are now working in Russian; or they did their undergraduate work in Arabic and are now working in French; or, especially frequent, they did their undergraduate work in Danish or Chinese or Romanian or Spanish and are now working in English.

All these transitions are difficult. I mean, one has read textbooks in a language and encountered H̃ and understood the mathematics, but that doesn't tell one to call the accent "s volnoi" (Russian) respectively "tilde" (English). Then when one *has* learned to say "aitch tilde" one may have the bad luck to work with a professor who says "aitch twiddle" instead.

But whatever the difficulties of doing research in an unfamiliar language—Russian or French or German—they are nothing to the near-impossibility of doing research in a language where the widely used letter "i" can stand not for a plain old vowel but for a sound that's almost two syllables, like "aa-ii." Mathematicians from all over the world agree in wonderment: How can anyone, even natives, overcome such an impediment to research? Some English words even have this preposterous pronunciation *twice*, like "finite"; then the language perversely reverses itself, as in "infinite "

Worst of all, there is one constant, spoken of daily by all of us, whose name is pronounced the same in all the world's mathematical languages *but* English, and in English it has that obnoxious vowel, so that Germans and Venezuelans and Greeks alike must offend their deepest linguistic instincts by making themselves say, "Paa-ii."

[1]See *Mathematical Intelligencer* vol 14, no 2, 51, vol 15, no 1, 5, vol 15, no 2, 26