CONTRIBUTIONS TO ALGEBRAIC NUMBER THEORY

TAMÁS SZAMUELY

If the publication year of Hilbert's *Zahlbericht* (1897) can be regarded as the birth date of algebraic number theory as a separate discipline, then the field was still at a tender age at the dawn of the 20th century. Nevertheless it was quickly introduced in Hungary thanks to the efforts of Gyula Kőnig. Hungarian mathematicians made significant contributions to the subject during the first decades of the century, but after the death of Kőnig there was no strong personality who would hold a research group together. This may explain the fact that work in the area gradually died out in the country, and it was only in the 1970s that it received new impetus through the emergence of a new research group in the city of Debrecen.

In the following we briefly review the number-theoretic work of four mathematicians: Kőnig, Kürschák, Bauer and Rédei. We are very grateful to Peter Roquette for his comments on a first version of this text.

Gyula Kőnig (1849–1913)

When discussing contributions of Hungarian mathematicians to algebraic number theory, the person to start with is undoubtably Gyula (Julius) Kőnig. Though in retrospect it now seems to us that his lasting contributions to mathematics were in the field of set theory and logic, his influence on arithmetic research is unquestionable. The two mathematicians who made the most significant contributions to algebraic number theory, József Kürschák and Mihály Bauer, were both his pupils, and he directly stimulated much of the work carried out by his assistants and colleagues.

Kőnig was a leading figure of Hungarian mathematics from the last quarter of the 19th century until the beginning of the 20th. He organized higher mathematical education in Budapest almost single-handedly. At the Technical University of Budapest he lectured for more than 30 years on virtually all important topics in contemporary mathematics. Besides serving as department head and later as university rector, he has also been appointed several times by the government to conduct reforms of secondary school education. During the last decade of his life he even found the time to serve as CEO of one of the largest Hungarian publishing houses, the Franklin Society.

His best known result in number theory is a necessary and sufficient criterion for the solvability of a polynomial equation of degree $p-2$ over $\mathbf{F}_p$. According to his criterion, the existence of a root is equivalent to the vanishing of the cyclic determinant (of rank $p-1$) built out of the coefficients of the polynomial. His theorem was extended and published by his student G. Rados [26].

Kőnig's main contribution to algebraic number theory is contained in his magnum opus *Einleitung in die allgemeine Theorie der algebraischen Größen* [16], first published in Hungarian in 1901. This thick volume was one of the first systematic developments of methods of abstract algebra, in the spirit of Kronecker whose lectures Kőnig had attended in Berlin in his youth. The last three chapters are devoted to Diophantine questions and the theory of algebraic integers. Though the book soon became obsolete through the intensive foundational work of the German algebraic school, it was highly influential in its time. For some aspects of its influence on the algebraic research of the period see [9].

József Kürschák (1864–1933)

Arguably the most important contribution by a Hungarian mathematician to the development of algebraic number theory is the 1913 paper [17] by József (Josef) KÜRSCHÁK. Remarkably, this is his only work on the subject, but it is also the work that won him international recognition when he presented its main results at the 1912 International Congress of Mathematicians in Cambridge. Otherwise Kürschák's carreer was fairly similar to that of its mentor Kőnig: he studied and later taught at the Technical University of Budapest, became full professor in 1904 and served as rector for three years. He was also much occupied with didactics; a mathematical contest for secondary schools he initiated together with Kőnig now bears his name.

The paper [17] is a masterpiece of mathematical writing, and still makes excellent reading almost a hundred years later. In it Kürschák introduces the fundamental notion of a *valuation* on a field K. This is a function $a \mapsto ||a||$ with nonnegative real values satisfying the following three axioms:

1. $||a|| = 0$ if and only if $a = 0$;
2. $||1 + a|| \leq 1 + ||a||$ for all $a \in K$;
3. $||ab|| = ||a|| \cdot ||b||$ for all $a, b \in K$.

Kürschák also imposes a nontriviality axiom requiring that the valuation takes at least one value other than 0 or 1. Below we shall tacitly assume that the valuation is nontrivial. A field equipped with a valuation is called a *valued field.* Using the multiplicativity axiom (3) one sees that axiom (2) is equivalent to the more familiar triangle equality $||a + b|| \leq ||a|| + ||b||$.

Examples of valuations are the usual real and complex absolute values, but also the *p-adic absolute value* on $\mathbf{Q}$ that Kürschák defines by the formula $||a||_p = e^{-r}$, where r is the unique integer for which one may write $a = (u/v)p^r$ with u and v integers prime to p. Here e is the basis of the natural logarithm, but in fact it could be any positive real number. This valuation satisfies the ultrametric property which is sharper than (2): one has $||a + b|| \leq \max(||a||, ||b||)$ for all $a, b \in K$.

In today's terminology, each valuation defines a norm on K and hence a metric, so one has a notion of convergence. One says that K is *complete* with respect to the valuation (Kürschák used the then prevalent term 'perfect' instead of 'complete') if every Cauchy sequence in K converges. The first main result of Kürschák is that each valued field K can be embedded as a dense valued subfield in a complete valued field, its *completion.* In the case of $K = \mathbf{Q}$ and the usual absolute value one obtains the field of real numbers, and Kürschák's construction is a direct generalisation of Cantor's construction of the reals by means of fundamental sequences. But he also remarks that his construction is a special case of one by F. Riesz [32] who, in today's terms, considered completions of metric spaces (in fact, the report of Riesz is rather sketchy).

The main new example is that of the completion of $\mathbf{Q}$ with respect to the p-adic valuation. Here Kürschák shows that the valued field obtained by his procedure is ismorphic to the field $\mathbf{Q}_p$ of p-adic numbers introduced a few years before by Kurt Hensel ([14], [15]). Hensel defined p-adic numbers formally by power series expansions of the shape $a_0p^r + a_1p^{r+1} + \cdots + a_np^{n+r} + \ldots$ with $r \in \mathbf{Z}$ and $a_i \in \{0, 1, \ldots, p-1\}$, and introduced explicit addition and multiplication rules on them. As Kürschák rightly remarked, the relationship between his construction and Hensel's is similar to the relationship between Cantor's construction of real numbers and decimal expansions. We may add that this dichotomy is very fruitful for number-theoretic considerations even at the present day.

From the above we can clearly see that both Cantor's ideas and recent developments in number theory were well immersed in Hungarian mathematical thinking at the time. Maybe it is not hasardous to guess that this was largely due to Kőnig's influence, whose own favourite fields were arithmetic and logic. In any case Kürschák was the right man at the right place.

Kürschák's paper contains not only the construction of completions, but also the proof of a fundamental theorem:

Every valued field can be embedded into a complete valued field that is algebraically closed.

More precisely, Kürschák shows that an algebraic closure $\overline{K}$ of a complete valued field K can be canonically equipped with a valuation extending that of K, and that the completion of $\overline{K}$ remains algebraically closed. In the case $K = \mathbf{Q}_p$ one obtains by this procedure the field that is nowadays denoted by $\mathbf{C}_p$; it is the p-adic analogue of the field of complex numbers. The importance of this field for current research in number theory cannot be overrated: it is the natural basis for the development of p-adic analysis, and in particular the theory of p-adic zeta and L-functions.

To construct the extension of the valuation to the algebraic closure $\overline{K}$, Kürschák observed that the most natural way is to put $||a|| := ||N(a)||^{1/n}$ for an element $a \in \overline{K}$ of degree n over K. Here N is the field norm from $K(a)$ to K; the element $N(a) \in K$ equals the constant term of the minimal polynomial of a up to a sign. With this definition the axioms (1) and (3) of a valuation can be easily checked, but (2) is more difficult. Kürschák remarked that in the case of an *ultrametric* valuation there is an easy proof using a direct generalisation of an observation of Hensel according to which if a monic *irreducible* polynomial over $\mathbf{Q}_p$ has a constant term of valuation at most 1, then all coefficients must have valuation at most 1. Hensel's observation in turn has a strong analogy with Weierstrass' factorization theory of power series, so accordingly Kürschák sought for inspiration in function theory in order to handle the general case. His proof is based on a generalisation of Hadamard's results on computing the convergence radius of a power series from its coefficients.

Today we do not need Kürschák's long proof any more, because in his 1917 papers [24] and [25] A. Ostrowski made further significant advances in the theory. He introduced the notion of *archimedean* valuations (those for which the powers of a nonzero element may have arbitrary high valuation), and proved that a complete archimedean valued field is isomorphic to either $\mathbf{R}$ or $\mathbf{C}$. Thus in this case the construction of a valuation on the algebraic closure is tautological. Ostrowski also observed that non-archimedean valuations are necessarily ultrametric, and hence Hensel's simple argument can be applied to extend the valuation. This approach, which is the standard one adopted today, is simpler than Kürschák's, but Kürschák's proof has the merit of being uniform. On the other hand, he does not seem to have observed the important fact that the extension of the valuation is *unique*.

Having extended the valuation to $\overline{K}$, Kürschák finally proved that the completion of $\overline{K}$ remains algebraically closed. He called this result the fundamental theorem of valuation theory, because in the case $K = \mathbf{R}$ it reduces to the fundamental theorem of algebra, viz. that $\mathbf{C}$ is algebraically closed. Accordingly, his way of proving the theorem was an adaptation of a method of Weierstrass for proving the fundamental theorem of algebra. He prudently left open the question whether $\overline{K}$

itself was already complete. This was settled in the negative by Ostrowski in his paper [23], published immediately after Kürschák's in the same volume of Crelle's Journal.

Today we regard Kürschák's paper as the founding work of valuation theory, but the author was very modest about it. At the end of the introduction he wrote that his investigations were 'almost without exception obvious generalisations of known theories'. Of course this was not so. But it may very well be that despite the favourable international reactions Kürschák was not fully aware of the importance of his results. One reason for this was that Hensel's theory of p-adic numbers took quite some time to obtain universal recognition. In his obituary of Hensel [13] Hasse paints a vivid picture of the unfavourable attitude of the leaders of the subject, from Hecke to Artin. The situation only changed in the 1930s when Hasse, Noether and others obtained major advances in class field theory using p-adic methods. But after his groundbreaking paper Kürschák did not return to the subject any more.

For further details and later developments we refer to the fascinating survey by Roquette [33].

Mihály Bauer (1874–1945)

Mihály (Michael) Bauer is the only Hungarian mathematician in the first half of the 20th century who contributed almost exclusively to algebraic number theory and related algebra. He was a pupil of Kőnig and Rados and, like his masters, taught at the Technical University of Budapest. But he never obtained full professorhip and was even forced to an early retirement in 1936, presumably partly for racial reasons. In contrast to this neglect in his own country he was held in esteem by leading mathematicians of the day including Hardy, Landau and van der Waerden, and he is the only Hungarian mathematician cited in Hasse's famous *Klassenkörperbericht*.

The most important contibutions of Bauer concern the decomposition of primes in number fields, with special emphasis on the Galois case. Recall that given a finite extension $K|\mathbf{Q}$ with ring of integers $\mathcal{O}_K$, the ideal $p\mathcal{O}_K$ of $\mathcal{O}_K$ generated by a prime number p decomposes as a product $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$, where the $\mathfrak{p}_i$ are exactly the prime ideals in $\mathcal{O}_K$ containing p. They are called the *prime divisors* of p in K. The degree of the field extension $\mathbf{F}_p \subset \mathcal{O}_K/\mathfrak{p}_i$ is called the *degree* of $\mathfrak{p}_i$. One says that p is *unramified* in K if $e_i = 1$ for all i. If moreover all the $\mathfrak{p}_i$ are of degree 1, then p is *completely split* in K.

The first significant result of Bauer concerning the splitting of primes in extensions appeared in his papers [2] and [3]. Here he proved:

Given two finite extensions K_1, K_2 of $\mathbf{Q}$, the set of primes that split completely in the composite field K_1K_2 equals, up to a finite number of *exceptions, the set of those primes that split completely both in* K_1 *and in* K_2*. Moreover, this set has density* $1/d$*, where* d *is the degree of the Galois closure of* K_1K_2 *over* $\mathbf{Q}$.

As an immediate corollary, one obtains:

If K_1 *and* K_2 *are two finite Galois extensions of* $\mathbf{Q}$ *such that, up to a finite number of exceptions, the same primes split completely in* K_1 *and in* K_2*, then* $K_1 = K_2$.

Nowadays we usually view these results as consequences of the famous density theorem of Chebotarev [35]. However, Bauer obtained them twenty years earlier.

The statement of the corollary is rather surprising. In fact, it answers in the Galois case a question raised by Kronecker about characterising number fields by the splitting behavior of primes. Kronecker called this a 'boundary value problem' (*Randwertproblem*) because of a (vague) analogy with Cauchy's theorem computing the values of an analytic function on a disc from its values taken at the boundary.

A perhaps even more striking theorem was discovered in the late 1960's by J. Neukirch [21]: *Given two finite Galois extensions* K_1, K_2 *contained in a fixed algebraic closure* $\overline{\mathbf{Q}}$*, the existence of an isomorphism of Galois groups* $\mathrm{Gal}\,(\overline{\mathbf{Q}}|K_1) \cong \mathrm{Gal}\,(\overline{\mathbf{Q}}|K_2)$ *forces* $K_1 = K_2$. The starting point of Neukirch's proof is Bauer's result above, which reduces the statement to a characterisation of decomposition and inertia groups of prime ideals in the Galois group. Neukirch did this using class field theory. Today we know that the theorem holds more generally for arbitrary finite extensions of $\mathbf{Q}$ (Neukirch, Uchida), and even for arbitrary fields finitely generated over the prime field (Pop). But the starting point of the whole development was Neukirch's paper [21] which exploited Bauer's result.

In 1916 Bauer obtained notable extensions of his earlier results. For a finite extension $K|\mathbf{Q}$ he considered the set $P(K)$ of primes unramified in K and having a prime divisor of degree 1. In the Galois case this is just the set of completely split primes, but in the non-Galois case there is a difference. In fact, his paper [4] contains the following remarkable observation: *a finite extension* $K|\mathbf{Q}$ *is Galois if and only if each prime in* $P(K)$ *splits completely in* K.

Concerning the sets $P(K)$ he showed in his paper [5]:

Let K *be a finite extension of* $\mathbf{Q}$*, and let* N *be a finite Galois extension. Then* $K \supset N$ *if and only if* $P(K) \subset P(N)$ *up to a finite number of exceptions.*

This result, the most famous one of Bauer, gives a final answer to Kronecker's question. Again it is nowadays derived from the Chebotarev density theorem (see [22], §VII.13), but the priority of Bauer is unquestionable. He himself used an earlier density theorem of Frobenius. The result holds more generally for extensions of an arbitrary number field instead of $\mathbf{Q}$, with essentially the same proof.

The papers [4] and [5] are the ones cited in the *Klassenkörperbericht* of Hasse. In his next article [6] and some later works Bauer pursued the study of the topic, obtaining more general results about the decomposition of (not necessarily split) prime ideals in composita of finite Galois extensions.

Bauer proved the above theorems by global methods, but (not surprisingly, given his environment) he was also among the first to recognize the power of the p-adic techniques introduced by Hensel. He wrote several papers about the relationship between local and global ramification theory, and in the joint paper [7] arising from correspondence with Chebotarev gave a simple p-adic proof of a then recent theorem of Ore. This theorem computes the ramification indices e_i and degrees f_i of the prime divisors of a prime p in a finite extension $K|\mathbf{Q}$ from the decomposition of the reductions of the defining polynomial of K modulo suitable powers of p.

Here we conclude this brief overview of Bauer's most lasting contributions. The very clear survey by Rédei [30] discusses Bauer's mathematical papers one by one. We now say a few words about Rédei's own work.

László Rédei (1900–1980)

The distinguished algebraist László Rédei started his carreer with number-theoretic investigations. After his first papers, which were devoted to new proofs of the quadratic reciprocity law, he focused his attention on a problem which was to occupy him during the next twenty years, namely the determination of the 2-primary part of the ideal class group Cl_K of a quadratic number field K. This is a finite abelian group which is a direct sum of cyclic groups of 2-power order. At the time he started working on the problem the only known result was the fact, going back to Gauss, that the number of cyclic components equals 2^{r-1}, where r is the number of distinct prime divisors of the discriminant D of K. This did not explain how large the cyclic components can be. Rédei was the first to obtain a formula on the number r_4 of those cyclic components which have order at least 4. Namely, he showed that 2^{r_4} equals the number of those product decompositions $D = D_0D_1$ where each D_i is again the discriminant of some quadratic number field (or equals 1), and moreover for each prime divisor p of D_i the integer D_{1-i} is a quadratic residue mod p ($i = 0, 1$). Soon afterwards H. Reichardt found a simpler proof of the formula, and after a first publication by Rédei in Hungarian they published the result in the joint paper [31].

In a long series of subsequent papers Rédei continued his exploration of the 2-primary part of the class group, culminating in the papers [28] and [29]. Here he described an algorithm that computes the 2-torsion part even for generalized ideal class groups defined using orders in the quadratic number field. For this he had to study the Artin symbol in towers of class fields of 2-power degree over the quadratic field K. As an application, he obtained conditions for the solvability of the Pell type Diophantine equations $x^2 - df^2y^2 = -1$, where d and f are squarefree integers with $(f, 2d) = 1$. His theory was later substantially simplified by Morton [20], who also gave a new short proof of the Rédei–Reichardt theorem.

In a series of papers published between 1936 and 1942 Rédei also investigated the problem of determining those real quadratic number fields $\mathbf{Q}(\sqrt{d})$ whose ring of integers is Euclidean. This was a question intensively studied in the 1930's and '40s by many number theorists, including Erdős, Heilbronn, Hua and, most importantly, Davenport. Today we know that there are exactly 21 such fields; their list can be found e.g. in later editions of the classic text by Hardy and Wright [11]. Rédei found several of them and showed that many others are not Euclidean. For the anecdote we may mention that he actually delayed the complete solution of the problem by a few years, because his 1942 paper [27] contained the erroneous claim that the field $\mathbf{Q}(\sqrt{97})$ is Euclidean. The mistake was only noticed ten years later by Barnes and Swinnerton-Dyer [1]. For a recent survey of the question see [8].

The obituaries [18] and [19] contain a complete list of Rédei's publications.

Later developments

During the decades following the work of Rédei described above, number-theoretic research in Hungary concentrated almost exclusively on elementary and analytic questions. It is only in the 1970's that a new, internationally recognized research group on Diophantine questions was created in the city of Debrecen under the leadership of Kálmán Győry. They have obtained significant effective finiteness results for solutions of Diophantine equations using methods of transcendental number theory. Another main focus of their research is on algorithmic aspects of algebraic number theory and explicit methods for Diophantine equations. Despite the untimely death of some of its members, the group is still very active and vigorous. Therefore according to the principles of the present volume we cannot discuss their work in detail, leaving the task to historians of the 22nd century.

References

[1] E. S. Barnes and H. P. F. Swinnerton-Dyer, The inhomogeneous minima of binary quadratic forms I, *Acta Math.* 87 (1952), 259–323.

[2] M. Bauer, Über einen Satz von Kronecker, *Arch. der Math. u. Phys. (3)* 6 (1903), 218–219.

[3] ______, Über zusammengesetzte Körper, *Arch. der Math. u. Phys. (3)* 6 (1903), 221–222.
[4] ______, Zur Theorie der arithmetischen Progression, *Arch. d. Math. u. Phys. (3)* **25** (1916), 131–134.
[5] ______, Zur Theorie der algebraischen Zahlkörper, *Math. Ann.* 77 (1916), 353–356.
[6] ______, Über zusammengesetzte Zahlkörper, *Math. Ann.* 77 (1916), 357-361.
[7] M. Bauer, N. Tschebotaröw, p-adischer Beweis des zweiten Hauptsatzes von Herrn Ore, *Acta Sci. Math. Szeged* **4** (1928), 56–57.
[8] R. B. Eggleton, C. B. Lacampagne and J. L. Selfridge, Euclidean quadratic fields, *Amer. Math. Monthly* 99 (1992), 829–837.
[9] J. Gray, König, Hadamard and Kürschák, and abstract algebra, *Math. Intell.* **19** (1997), 61–64.
[10] K. Győry, Rédei's work in number theory (Hungarian), unpublished manuscript.
[11] G. H. Hardy, E. M. Wright, *An introduction to the theory of numbers*, 5th edition, Oxford University Press, 1979.
[12] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Teubner, Leipzig, 1930.
[13] ______, Kurt Hensel zum Gedächtnis, *J. reine angew. Math.* **187** (1949), 1–13.
[14] K. Hensel, Über die arithmetischen Eigenschaften der Zahlen I, II, III, *Jber. Deutsche Math. Ver.* 16 (1907), 299-319, 388-393, 473-496.
[15] ______, *Theorie der algebraischen Zahlen*, Teubner, Leipzig, 1908.
[16] J. König, *Einleitung in die allgemeine Theorie der algebraischen Größen*, Teubner, Leipzig, 1903.
[17] J. Kürschák, Über Limesbildung und allgemeine Körpertheorie, *J. reine angew. Math.* **142** (1913), 211–253.
[18] L. Márki, A tribute to L. Rédei, *Semigroup Forum* 32 (1985), 1–21.
[19] L. Márki, O. Steinfeld and J. Szép, Short review of the work of László Rédei, *Studia Sci. Math. Hungar.* **16** (1981), 3–14.
[20] P. Morton, On Rédei's theory of the Pell equation, *J. reine angew. Math.* 307/308 (1979), 373–398.
[21] J. Neukirch, Kennzeichnung der p-adischen und der endlichen algebraischen Zahlkörper, *Invent. Math.* 6 (1969), 296–314.
[22] ______, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften, vol. 322, Springer, Berlin, 1999.
[23] A. Ostrowski, Über einige Fragen der allgemeinen Körpertheorie, *J. reine angew. Math.* 148 (1913), 255–284.
[24] ______, Über sogenannte perfekte Körper, *J. reine angew. Math.* 147 (1917), 191–204.
[25] ______, Über einige Lösungen der Funktionalgleichung $\varphi(x) \cdot \varphi(y) = \varphi(xy)$, *Acta Math.* 41 (1917), 271–284.
[26] G. Raussnitz (Rados), Zur Theorie der Congruenzen höheren Grades, *J. reine angew. Math* **90** (1886), 258–260.
[27] L. Rédei, Zur Frage des Euklidischen Algorithmus in quadratischen Zahlkörpern, *Math. Ann.* 118 (1942). 588–608.
[28] ______, Bedingtes Artinsches Symbol mit Anwendung in der Klassenkörpertheorie, *Acta Math. Acad. Sci. Hungar.* 4 (1953). 1–29.
[29] ______, Die 2-Ringklassengruppe des quadratischen Zahlkörpers und die Theorie der Pellschen Gleichung, *Acta Math. Acad. Sci. Hungar.* 4 (1953). 31–87.
[30] ______, Life and work of Mihály Bauer (Hungarian), *Mat. Lapok* **4** (1953). 241–262.

[31] L. Rédei, H. Reichardt, H, Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers, *J. reine angew. Math.* 170 (1933), 69–74.

[32] F. Riesz, Stetigkeit und abstrakte Mengenlehre, *Atti del congresso int. dei Mathematici (Roma, 6–11 aprile 1908)*, vol. 2, 18–24.

[33] P. Roquette, History of valuation theory I, in *Valuation theory and its applications I*, Fields Inst. Commun., 32, Amer. Math. Soc., Providence, 2002, 291–355,

[34] B. Szénássy, Gyula Kőnig (1849–1813) (Hungarian), Akadémiai Kiadó, Budapest, 1965.

[35] N. Tschebotareff, Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören, *Math. Ann.* 95 (1925), 191–228.