Snapshots of modern mathematics
from Oberwolfach

№ 12/2017

Solving quadratic equations in many variables

Jean-Pierre Tignol[1]

Fields are number systems in which every linear equation has a solution, such as the set of all rational numbers $\mathbb{Q}$ or the set of all real numbers $\mathbb{R}$. All fields have the same properties in relation with systems of linear equations, but quadratic equations behave differently from field to field. Is there a field in which every quadratic equation in five variables has a solution, but some quadratic equation in four variables has no solution? The answer is in this snapshot.

1 Fields

No problem is more fundamental to algebra than solving polynomial equations. Indeed, the name *algebra* itself derives from a ninth century treatise [1] where the author explains how to solve quadratic equations like $x^2 + 10x = 39$. It was clear from the start that some equations with integral coefficients like $x^2 = 2$ may not have any integral solution. Even allowing positive and negative numbers with infinite decimal expansion as solutions (these numbers are called *real numbers*), one cannot solve $x^2 = -1$ because the square of every real number is positive or zero. However, it is only a small step from the real numbers to the solution

[1] Jean-Pierre Tignol acknowledges support from the Fonds de la Recherche Scientifique (FNRS) under grant n° J.0014.15. He is grateful to Karim Johannes Becher, Andrew Dolphin, and David Leep for comments on a preliminary version of this text.

of every polynomial equation: one gives the solution of the equation $x^2 = -1$ (or $x^2 + 1 = 0$) the name i and defines *complex numbers* as expressions of the form $a + bi$, where a and b are real numbers. This formal process is called *adjoining a zero* of the polynomial $x^2 + 1$ to the real numbers .

A famous result due to the German mathematician Carl Friedrich Gauss (1777–1855) asserts that every polynomial equation (of any positive degree[2]) with complex numbers as coefficients has a solution that is a complex number. This is known as the *Fundamental Theorem of Algebra*, even though every proof involves some argument from analysis because the very definition of real numbers is based on an approximation process.

Thus, whether it is possible to solve an equation depends on the numbers that are considered acceptable solutions. To discuss this type of question, one selects a set F of elements (usually numbers, but not always, as we will see later) on which one can operate with an addition and a multiplication satisfying the same rules as when one operates with integers, such as, for example, the distributive property. If F contains at least two distinct elements 0 and 1, and if every equation of the form $ax + b = 0$ for a, b in F with $a \neq 0$ has a solution in F, then the set F is said to be a *field*. Examples include the set $\mathbb{Q}$ of *rational* numbers, which are quotients of integers, the set $\mathbb{R}$ of real numbers, and the set $\mathbb{C}$ of complex numbers, but *not* the set $\mathbb{Z}$ of (positive and negative) integers, since for instance $2x + 3 = 0$ has no solutions in $\mathbb{Z}$ even though the coefficients 2 and 3 belong to $\mathbb{Z}$.

The idea of a field emerged during the 19th century from the consideration of examples more exotic than $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. For instance, one may consider a set consisting just of 0 and 1, and define an addition by setting $1+1 = 0$. (The other sums $0+0 = 0$, $0+1 = 1+0 = 1$, and the multiplications $0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0$ and $1 \cdot 1 = 1$ are given by the rules in the integers.) This set is just like $\mathbb{Z}$ in which one would have decided that $2 = 0$ (and therefore $4 = 0$ since $4 = 2 \cdot 2$, and $-11 = 1$ since $-11 = 2 \cdot (-6) + 1$, etc.); it is a field denoted by $\mathbb{F}_2$. More generally, if p is a prime integer, one can identify p with 0 in $\mathbb{Z}$ and obtain a field with p elements 0, 1, …, $p - 1$, which is denoted by $\mathbb{F}_p$. Note that in contrast to the other fields we have seen so far, $\mathbb{F}_p$ contains only finitely many elements; in other words, it is an example of a *finite field*.

Quiz 1: Do we obtain a field with 4 *elements by deciding that* $4 = 0$ *in* $\mathbb{Z}$ *(but* $2 \neq 0$*)?*

The examples above illustrate general procedures that can be used to produce a wealth of examples of fields with various properties. Just like the field $\mathbb{Q}$ is obtained from $\mathbb{Z}$ by forming fractions $\frac{a}{b}$ with a, b in $\mathbb{Z}$ (and $b \neq 0$), we

[2] The *degree* of a polynomial is its largest exponent. For example, the polynomial $4x^3 + x - 5$ has degree 3.

can start with a field F of our choice and build a new field by considering fractions $\frac{f(t_1,\ldots,t_n)}{g(t_1,\ldots,t_n)}$ where $f(t_1,\ldots,t_n)$ and $g(t_1,\ldots,t_n)$ are polynomials in n variables t_1, …, t_n with coefficients in F (and $g(t_1,\ldots,t_n) \neq 0$). The field thus obtained is known as the field of *rational functions* in the variables t_1, …, t_n over F; it is denoted by $F(t_1,\ldots,t_n)$. But there is more: before forming fractions, we can decide to identify with zero all the polynomials that are multiples of a given polynomial $p(t_1,\ldots,t_n)$. To be precise, the polynomial $p(t_1,\ldots,t_n)$ has to be *irreducible*, that is, it is not the product of two nonconstant polynomials with coefficients in F. This condition is an analogue to the requirement that p be a prime number in the construction of $\mathbb{F}_p$. Along with F, the resulting field contains n elements u_1, …, u_n related by the condition that $p(u_1,\ldots,u_n) = 0$. Roughly speaking, we have enlarged F by formally adjoining a zero of the polynomial $p(t_1,\ldots,t_n)$.

Quiz 2: What do we obtain if we start with $F = \mathbb{R}$ and apply this construction to polynomials in one variable t with $p(t) = t^2 + 1$?

2 Quadratic algebra versus linear algebra

Mathematicians designate by *linear algebra* the branch of algebra that deals with the solution of systems of equations of degree 1 in an arbitrary number of variables. Remarkably, the basic results of linear algebra hold over every field: solving a system of linear equations involves the same theoretical aspects and procedures whether the coefficients are complex or real numbers, or in a finite field like $\mathbb{F}_p$. For equations of degree higher than 1, the situation is completely different, and we may try to distinguish fields based on which equations have solutions. The field $\mathbb{C}$ is among the simplest in this respect, because *all* equations (barring "constant" equations like $1 = 0$) have solutions. In the 1950s, Serge Lang[3] had the insight to consider polynomial equations in more than one variable [6]. Similar as for polynomials in one variable, one can also define the *degree* of a polynomial in several variables; summing first over all exponents in each summand of a polynomial, one calls the highest of these sums the degree of the polynomial. For instance, the polynomial $x_1^5 \cdot x_2^3 - 2x_1 \cdot x_2^2$ has degree $5 + 3 = 8$. A polynomial is called *homogeneous* if all its summands have the same degree. Every homogeneous polynomial has a *trivial zero*; this is when all its variables are set to 0. Every other zero of a homogeneous polynomial is called nontrivial. Note that every polynomial can be turned into a homogeneous polynomial by using an additional indeterminate to raise the degree of each

[3] The French-born American mathematician Serge Lang (1927–2005) is not only known for his mathematical achievements, but also for his political activism and his role in a public controversy with the political scientist Samuel P. Huntington.

summand to the maximal degree. For instance, the polynomial $x_1^5x_2^3 - 2x_1x_2^2$ can be homogenized into $x_1^5x_2^3 - 2x_1x_2^2x_3^5$. The homogenized polynomial with $x_3 = 1$ plugged in has exactly the same zeros as the initial polynomial. Thus, restricting to homogeneous polynomials does not entail any significant loss of generality, and actually has some technical advantages.

Lang proposed the following definition relating the degree and the number of variables:

Definition. Let n be a nonnegative integer. A field F satisfies the *C_n-property* if for every positive integer $d > 0$, every homogeneous polynomial of degree d in at least $d^n + 1$ variables with coefficients in F has a nontrivial zero. If F satisfies the C_n-property, we also say that it is a *C_n-field.*

With this definition, the field $\mathbb{C}$ has the C_0-property; this follows directly from the Fundamental Theorem of Algebra. Some results that predate Lang's definition can be stated conveniently with this notation: Chiungtze C. Tsen proved that the field $\mathbb{C}(t)$ of rational functions in one variable over $\mathbb{C}$ satisfies the C_1-property, and by a result by Claude Chevalley and Ewald Warning every finite field is also a C_1-field. Lang extended Tsen's result by showing that the field of rational functions $F(t)$ in one variable over a C_n-field F has property C_{n+1}; but proving that a given field has property C_n may be extremely difficult because one needs to consider homogeneous polynomials of all degrees. (See [3] for a detailed discussion of the C_n-property.)

By restricting to homogeneous polynomials of degree 2 (which are simply called *quadratic forms*), Irving Kaplansky introduced in [4] a more manageable notion:

Definition. The *u-invariant* of a field F is the smallest integer u such that every quadratic form in at least $u + 1$ variables with coefficients in F has a nontrivial zero, or ∞ if no such integer exists. We write $u(F)$ for the u-invariant of F.

Thus, by definition $u(F) \leq 2^n$ if F is a C_n-field. In particular $u(\mathbb{C}) = 1$, and from the Chevalley–Warning theorem it is not difficult to derive that $u(\mathbb{F}_p) \leq 2$ for every prime p. Similarly, one can use the Tsen–Lang theorem to see that $u\big(\mathbb{C}(t_1, \ldots, t_n)\big) \leq 2^n$ for every $n \geq 0$. In fact, even the equalities $u(\mathbb{F}_p) = 2$ and $u\big(\mathbb{C}(t_1, \ldots, t_n)\big) = 2^n$ are true in these cases; but to show that "$\geq$" holds, it suffices to give an example of a form in 2^n variables that has only the trivial zero, which is not too difficult.

On the other hand, since for all $n \geq 1$ the quadratic form $x_1^2 + \cdots + x_n^2$ does not have any nontrivial zero in $\mathbb{R}$, it follows that $u(\mathbb{R}) = \infty$, and also $u(\mathbb{Q}) = \infty$.

Quiz 3: Find a quadratic form in two variables over $\mathbb{F}_2$ or $\mathbb{F}_3$ that does not have any nontrivial zero. Find a quadratic form in four variables over $\mathbb{C}(t_1, t_2)$ that does not have a nontrivial zero.

Since quadratic forms are much better understood than homogeneous polynomials of degree $d > 2$, one may expect that computing the u-invariant of a field would be much easier than establishing the C_n-property for some n. It is true that a few results are known on the u-invariant, but its computation is still surprisingly difficult. In the next sections, we discuss recent advances on two questions:

- Given an integer n, find a field F with $u(F) = n$.
- Given a field F with $u(F)$ known, compute $u\big(F(t)\big)$.

We will use the standard terminology inspired by geometry: the number of variables is the *dimension* of a quadratic form, and a quadratic form is *isotropic* if it has a nontrivial zero (and *anisotropic* otherwise). Thus, $u(F) = n$ means that there exists an n-dimensional quadratic form with coefficients in F that is anisotropic, and that every quadratic form of dimension $n + 1$ over F is isotropic.

Quiz 4: Show that if every quadratic form of dimension n is isotropic over a given field F, then also every quadratic form of dimension $n + 1$ is isotropic over F.

3 Fields with prescribed u-invariant

As we saw in the last section, $u\big(\mathbb{C}(t_1, \dots, t_n)\big) = 2^n$ for every $n \geq 0$. On the other hand, it is not too difficult to see that the u-invariant of a field cannot take the values 3, 5, or 7. In spite of the scarcity of examples of fields whose u-invariant he could compute, Kaplansky boldly conjectured that $u(F)$ is either ∞ or a power of 2 for every field F.

This was disproved by Alexander Merkurjev in 1988. In a short piece of work, which surprised all the specialists of quadratic forms, Merkurjev produced a field with u-invariant 6. He used the following amazing construction, which is described in detail in [5, Ch. 13] and [2, §38]. Start with a field F_0 and an anisotropic quadratic form q_0 of dimension 6 over F_0. The idea is to enlarge F_0 by adjoining formally a zero of every 7-dimensional quadratic form to F_0. For this, we need to consider the collection of all quadratic forms in 7 variables over F_0. For each of these forms $p(t_1, \dots, t_7)$, we apply in turn the procedure sketched at the end of Section 1. At the end, we obtain a field F_1 over which all the 7-dimensional quadratic forms *with coefficients in* F_0 are isotropic; but there may be 7-dimensional quadratic forms *over* F_1 that are not isotropic. Therefore, we repeat the construction with the collection of 7-dimensional quadratic forms over F_1, and obtain a field F_2 where all of these have a nontrivial zero. Repeating the same construction again and again, we obtain an increasing sequence of fields F_0, F_1, F_2, ... It makes sense to consider the limit (or union) F_∞ of this

series: it consists of all the elements that lie in at least one of the fields F_i (and hence also in F_j for all $j > i$). Now, let φ be a 7-dimensional quadratic form with coefficients in F_∞. For n large enough, all the coefficients of φ lie in F_n; but then F_{n+1} contains a nontrivial zero of φ, hence F_∞ contains a nontrivial zero of φ. Thus, $u(F_\infty) \leq 6$. The delicate part is of course to prove that the u-invariant of F_∞ is exactly 6 and not less. For this, Merkurjev makes a particular choice of the quadratic form q_0 over F_0, and he shows that q_0 remains anisotropic when one adjoins a zero to any quadratic form in 7 variables. Thus, q_0 remains anisotropic throughout the series of fields F_1, F_2, ..., hence also over F_∞. Therefore, $u(F_\infty) = 6$.

Merkurjev soon found a way to define quadratic forms of any even dimension $2n$ that remain anisotropic when a zero of a quadratic form of higher dimension is formally adjoined to the original field. His construction could then be modified to yield fields F with $u(F) = 2n$ for any integer n. The same iterative construction was used again in 2001 by Oleg Izhboldin to construct a field with u-invariant 9, and most recently by Alexander Vishik in 2009 to yield a field F with $u(F) = 2^r + 1$ for an arbitrary integer $r \geq 3$. To this date, whether there exists a field with an odd u-invariant that is not of the form $2^r + 1$ is an open problem. Because Merkurjev's construction yields huge intimidating fields, another intriguing problem is to construct fields of rational expressions in a *finite* number of elements with a u-invariant that is not a power of 2.

Quiz 5: Show that the quadratic form $x_1^2 + x_2^2 + x_3^2$ becomes isotropic when a zero of the quadratic form $x_1^2 + x_2^2 + x_3^2 + x_4^2$ is adjoined to $\mathbb{R}$.

4 Computing the u-invariant

Fields of rational functions in one variable are well understood from various viewpoints, but they still present challenging problems in terms of quadratic forms. The Tsen–Lang theorem, which shows that for every C_n-field F the field $F(t)$ has the C_{n+1}-property, suggests that $u\big(F(t)\big) = 2u(F)$ might hold for every field F. This is easy to prove if F is a C_n-field with $u(F) = 2^n$. Hence, for instance, $u\big(\mathbb{F}_p(t_1, \ldots, t_n)\big) = 2^{n+1}$ for every prime p and any number n of variables. But the property does not hold in general: David Leep showed me an example of a field F with $u(F) = 1$ and $u\big(F(t)\big) \geq 4$. And for an arbitrary field F with finite u-invariant we still do not even know whether $u\big(F(t)\big)$ is finite.

Substantial progress has been made in the last few years for special kinds of fields F, which are obtained from the field $\mathbb{Q}$ of rational numbers by an approximation procedure. If we talk about approximation, we have to specify how we want to measure distance. Real numbers are constructed from rational numbers by successive approximations for the usual notion of distance. But for every prime p we can define a distance between rational numbers for which

the sequence p, p^2, p^3, ... decreases to zero. If we use this distance instead of the usual one, the approximation procedure that produces real numbers in the usual case now yields new numbers called *p-adic numbers*. These numbers form a field denoted by $\mathbb{Q}_p$, which was first considered by Kurt Hensel around 1897. Fields of p-adic numbers have proven extremely useful in number theory. The field $\mathbb{Q}_p$ has a close connection with the finite field $\mathbb{F}_p$, from which one can prove that $u(\mathbb{Q}_p) = 4$. Emil Artin conjectured in the early 30s that $\mathbb{Q}_p$ has the C_2-property, but this conjecture turned out to be false, hence we cannot use the Tsen–Lang theorem to derive that $u\big(\mathbb{Q}_p(t)\big) = 8$. It was a major breakthrough when Raman Parimala and Venapally Suresh proved in 2008 that indeed $u\big(\mathbb{Q}_p(t)\big) = 8$ for $p \neq 2$. (Another proof was found shortly after by David Harbater, Julia Hartmann, and Daniel Krashen.) Using profound results in the analytic study of systems of quadratic forms over p-adic fields due to Roger Heath-Brown, in 2013 David Leep was able to remove the restriction on p and to show that $u\big(\mathbb{Q}_p(t_1, \ldots, t_n)\big) = 2^{n+2}$ for any prime p and any number n of variables. In spite of this important result, there are still basic questions about the u-invariant of fields of rational functions that remain open.

Hints for solving the quizzes

Quiz 1: Does the equation $2x + 1 = 0$ have a solution?

Quiz 2: This construction is a more involved description of the complex numbers $\mathbb{C}$, compare the first paragraph of this snapshot.

Quiz 3: Does the quadratic form $x_1^2 + x_1x_2 + x_2^2$ have a nontrivial zero over $\mathbb{F}_2$? How about the quadratic form $x_1^2 + x_2^2$ over $\mathbb{F}_3$?

For the last part of the quiz, you may in a first step try to find a quadratic form in two variables over $\mathbb{C}(t_1)$ without a nontrivial zero, like $t_1x_1^2 + x_2^2$. Let us check that indeed there cannot be a nontrivial solution of the equation $t_1x_1^2 + x_2^2 = 0$ over $\mathbb{C}(t_1)$: no matter what rational functions $f(t_1)$ and $g(t_1)$ we plug in for the variables x_1 and x_2, the degree of the enumerator of $t_1 \cdot f(t_1)^2$ is always odd, while the degree of the enumerator of $g(t_1)^2$ is always even, so these two terms can never add up to zero. In a similar spirit, you may now try to show that $t_2(t_1x_1^2 + x_2^2) + t_1x_3^2 + x_4^2$ has no nontrivial zero over $\mathbb{C}(t_1, t_2)$.

Quiz 4: Consider a quadratic form $p(x_1, \ldots, x_{n+1})$ of dimension $n + 1$ over the field F. There are two possible cases: if plugging in $x_{n+1} = 0$ yields a quadratic form of dimension n, then by our assumption this quadratic form has a nontrivial zero, say $(u_1, \ldots, u_n)$. Then $(u_1, \ldots, u_n, 0)$ is a nontrivial zero of the quadratic form $p(x_1, \ldots, x_{n+1})$. If, on the other hand, plugging $x_{n+1} = 0$ into $p(x_1, \ldots, x_{n+1})$ yields a quadratic form of dimension lower than n, this means that at least one variable x_i only appears in terms which also contain x_{n+1}. So $(0, \ldots, 0, x_i = 1, 0, \ldots, 0)$ is a nontrivial zero of $p(x_1, \ldots, x_{n+1})$.

Quiz 5: Note that if $x_1^2+x_2^2+x_3^2+x_4^2 = 0$, then $(x_1x_3 - x_2x_4)^2+(x_1x_4 - x_2x_3)^2+\left(x_3^2 + x_4^2\right)^2 = 0$.

References

[1] Mohammed ben Musa, *The algebra of Mohammed ben Musa*, Cambridge Library Collection, Cambridge University Press, Cambridge, 2013, Translated by Friedrich August Rosen, reprint of the 1831 edition.

[2] Richard Elman, Nikita Karpenko, and Alexander Merkurjev, *The algebraic and geometric theory of quadratic forms*, Society Colloquium Publications, vol. 56, American Mathematical Society, Providence, RI, 2008.

[3] Marvin J. Greenberg, *Lectures on forms in many variables*, W. A. Benjamin, Inc., New York-Amsterdam, 1969.

[4] Irving Kaplansky, *Quadratic forms*, Journal of the Mathematical Society of Japan **5** (1953), 200–207.

[5] T. Y. Lam, *Introduction to quadratic forms over fields*, Graduate Studies in Mathematics, vol. 67, American Mathematical Society, Providence, RI, 2005.

[6] Serge Lang, *On quasi algebraic closure*, Annals of Mathematics (2) **55** (1952), 373–390.

Jean-Pierre Tignol *is a professor of algebra at the Université catholique de Louvain (Belgium).*

Mathematical subjects
Algebra and Number Theory

DOI
10.14760/SNAP-2017-012-EN

Snapshots of modern mathematics from Oberwolfach provide exciting insights into current mathematical research. They are written by participants in the scientific program of the Mathematisches Forschungsinstitut Oberwolfach (MFO). The snapshot project is designed to promote the understanding and appreciation of modern mathematics and mathematical research in the interested public worldwide. All snapshots are published in cooperation with the IMAGINARY platform and can be found on www.imaginary.org/snapshots and on www.mfo.de/snapshots.

Junior Editors
Sophia Jahns and Anja Randecker
junior-editors@mfo.de

Senior Editor
Carla Cederbaum
senior-editor@mfo.de

Mathematisches Forschungsinstitut
Oberwolfach gGmbH
Schwarzwaldstr. 9–11
77709 Oberwolfach
Germany

Director
Gerhard Huisken

Mathematisches
Forschungsinstitut
Oberwolfach

IMAGINARY
open mathematics