CHAPTER 8

Integrable systems and number theory

Peter H. van der Kamp, Jan A. Sanders and Jaap Top

1. Introduction

The evolution equation

$$u_t = u_3 + uu_1 \text{ (KdV)},$$

where u_n is the n^{th} derivative of $u(x,t)$ with respect to x, was derived to describe water waves in shallow channels [**KdV95**]. It bears the names of Korteweg and de Vries and has become *the* prototype integrable nonlinear partial differential equation since the work in [**Miu68, MGK68, SG69, Gar71, KMGZ70, GGKM74**]. The KdV equation is for the field of *integrability* what the harmonic oscillator is for quantum mechanics: the system for which every method works. KdV has infinitely many conservation laws, infinitely many (co)symmetries, it has (co)symplectic and recursion operators, a Lax-pair, a bilinear form, the Painlevé property, stable local solutions and it can be solved by the inverse scattering method.

Once all these properties are established, the obvious next question is: are there more equations like this? The goal we have in mind is the classification of 'integrable' partial differential equations. A few choices have to be made here, for instance, what kind of equations are to be classified and what exactly will be our definition of integrability. We will focus on the existence of infinitely many generalized symmetries (a precise definition follows in the next section).

We limit ourselves to polynomial equations, mainly because for these the symbolic calculus can be used. For classification results in the general case we refer to [**Zak91**], in particular [**MŠS91**]. We remark here that these lists give a different kind of classification, since they allow for much larger classes of transformations. Contrary to our analysis they can only classify one order at the time and cannot exclude the possibility that higher order equations are integrable. The classification results given here, which are based on the thesis of Jing Ping Wang [**Wan98**], and following publications, do allow, at least in the scalar case, a complete classification up till all orders. This breakthrough was made possible by the use of the symbolic method and the subsequent application of number theoretic and algebraic geometric methods and gives us an extremely elegant application of pure mathematics. As an illustration of the impact of this kind of theory, let us mention the fact that only a decade ago it was perfectly legitimate to publish papers on the search of integrable seventh and ninth order scalar polynomial equations, cf. [**Ger96, Ger93, GKZ90**]. The present results show why these efforts were all in vain.

2. Scalar equations

2.1. Generalized symmetries. Let $K(u)$ and $S(u)$ be functions of $u = u_0$ and a finite number of its derivatives $u_i = \frac{\partial^i u}{\partial x^i}$. The function $S(u)$ is called a *generalized symmetry* of the equation $u_t = K(u)$ if $v = u + \varepsilon S(u)$ satisfies $v_t = K(v) + \mathcal{O}(\varepsilon^2)$. The word 'generalized' is included in this definition to stress the fact that S in principle depends not only on u, but also on some of its derivatives u_i.

A completely algebraic description of this notion, limited to polynomial equations, is obtained as follows. Write $\mathcal{R} := \mathbb{C}[u, u_1, u_2, \ldots]$ for the polynomial ring in infinitely many variables $u = u_0, u_1, u_2, \ldots$ and let $f \in \mathcal{R}$. Write D_x for the derivation on $\mathcal{R}$ defined by $D_x(u_i) = u_{i+1}$ for all $i \geq 0$. Then

$$D_x(f) = \sum_{n \geq 0} u_{n+1} \frac{\partial f}{\partial u_n}.$$

Denote by δ_f the unique derivation on $\mathcal{R}$ satisfying $\delta_f(u) = f$ and $\delta_f \circ D_x = D_x \circ \delta_f$. This operator can (formally) be written as

$$\delta_f = \sum_{n \geq 0} D_x^n(f) \frac{\partial}{\partial u_n}.$$

This derivation δ_f is the prolongation of the evolutionary vectorfield with characteristic f, cf. [**Olv93**, equation 5.6]. Also, $\delta_f(g) = D_g(f)$, where D_g is the Fréchet derivative of g, cf. [**Olv93**, proposition 5.25].

Extend δ_f to a derivation on the dual numbers $\mathcal{R}[\varepsilon]$ (with $\varepsilon^2 = 0$) by $\delta_f(g + \varepsilon h) = \delta_f(g) + \varepsilon \delta_f(h)$ for $g, h \in \mathcal{R}$. With these notations, $S \in \mathcal{R}$ is a generalized symmetry of $K \in \mathcal{R}$ (or, of the equation $u_t = K(u, u_1, u_2, \ldots)$), if

$$\delta_K(u + \varepsilon S) = K(u + \varepsilon S, u_1 + \varepsilon D_x(S), \ldots, u_i + \varepsilon D_x^i(S), \ldots).$$

We have for arbitrary $S, K \in \mathcal{R}$ that

$$\begin{aligned}
\delta_K(u + \varepsilon S) &= \delta_K(u) + \varepsilon \delta_K(S) \\
&= K(u) + \varepsilon \delta_K(S) \\
&= K(\ldots, u_i + \varepsilon D_x^i S, \ldots) - \varepsilon \textstyle\sum_i \frac{\partial K}{\partial u_i} D_x^i S + \varepsilon \delta_K(S) \\
&= K(\ldots, u_i + \varepsilon D_x^i(S), \ldots) + \varepsilon(\delta_K S - \delta_S K).
\end{aligned}$$

Hence S is a generalized symmetry of the equation $u_t = K(u, u_1, \ldots)$ precisely when the Lie bracket $[K, S] = \delta_K S - \delta_S K$ vanishes.

If one writes φ_f for the automorphism of $\mathcal{R}[\varepsilon]$ which sends $g + h\varepsilon$ to $g + (h + \delta_f(g))\varepsilon$, then yet another way to define a symmetry S of K is by demanding that $\varphi_S(K) = \varphi_K(S)$.

Note that the bracket defined here is indeed a Lie bracket on $\mathcal{R}$, i.e., it is bilinear and it satisfies $[f, f] = 0$ and $[[f, g], h] + [[g, h], f] + [[h, f], g] = 0$. One way to verify this, is by noting that $\delta_{[f,g]} = \delta_f \circ \delta_g - \delta_g \circ \delta_f$ is the standard Lie bracket of δ_f and δ_g in the Lie algebra of all derivations on $\mathcal{R}$. As usual for $f \in \mathcal{R}$ the linear operator $g \mapsto [f, g]$ is called the adjoint of f and it is written as ad(f). The set of generalized symmetries of $u_t = K(u, u_1, \ldots)$ is precisely the kernel of ad(K). Note that by the general theory of Lie algebras, these generalized symmetries of K also form a Lie algebra (with the same Lie bracket).

DEFINITION 2.1. An equation $u_t = K$ is called *integrable* if the space of generalized symmetries of K is infinite dimensional (over $\mathbb{C}$), and *almost integrable of depth (at least, at most)* n if the space of generalized symmetries of K is exactly (at least, at most) n-dimensional. When an equation is almost integrable but not integrable we say that it is *almost integrable of finite depth*.

EXAMPLE 2.2. For any equation $u_t = K(u)$, the functions u_1 and $K(u)$ are generalized symmetries as is easily verified. $\mathbb{C}$-linear combinations of u_1 and $K(u)$ are called trivial symmetries; all other ones nontrivial.

EXAMPLE 2.3. A nontrivial symmetry of the KdV equation $u_t = u_3 + uu_1$ is

$$u_5 + \frac{5}{3}uu_3 + \frac{10}{3}u_1u_2 + \frac{5}{6}u^2u_1,$$

as can be verified by a tedious but straightforward calculation. In the next section we will explain how one may find such a symmetry.

2.2. λ-homogenuity and grading. One associates *weights* to the monomials in $\mathcal{R}$ by fixing some $\lambda \in \mathbb{R}$ and assigning to the monomial $u_{i_0} \cdots u_{i_r}$ the weight $r\lambda + i_0 + \ldots + i_r$. If every monomial in K has the same weight, then the equation $u_t = K$ is called *λ-homogeneous*. Note that this depends on the choice of λ; for example, in the KdV equation one has $K(u) = u_3 + uu_1$ with two monomials of weight 3 and $\lambda + 1$, respectively. Hence only with the choice $\lambda = 2$ this equation is λ-homogeneous (of weight 3). One sees that with this choice, also the symmetry $u_5 + \frac{5}{3}uu_3 + \frac{10}{3}u_1u_2 + \frac{5}{6}u^2u_1$ is λ-homogeneous, of weight 5. In these cases the weight equals the *order*, which is by definition the highest n such that u_n occurs in the expression.

We now discuss how to find symmetries in the case that $K(u)$ is λ-homogeneous. A calculation with the Lie bracket $[u_{i_0}\cdots u_{i_r}, u_{j_0}\cdots u_{j_s}]$ shows that if $f, g \in \mathcal{R}$ are λ-homogeneous of weights w and w' respectively, then $[f, g]$ is λ-homogeneous of weight $w + w'$. It follows that if K is λ-homogeneous and S is a symmetry of K, then the λ-homogeneous parts of S are symmetries of K as well. This reduces the problem of finding all symmetries of a λ-homogeneous equation to the problem of finding all λ-homogeneous symmetries. Next, one puts a *grading* on the Lie algebra $\mathcal{L} := \{f \in \mathcal{R} | f(0, 0, \ldots) = 0\}$ (with the Lie bracket $[f, g] = \delta_g f - \delta_f g$). This means we write it as a direct sum

$$\mathcal{L} = \mathcal{L}^0 \oplus \mathcal{L}^1 \oplus \cdots$$

of linear subspaces in such a way that $[\mathcal{L}^i, \mathcal{L}^j] \subset \mathcal{L}^{i+j}$ for all i, j. This is done by defining $\mathcal{L}^j$ (for $j \geq 0$) to be generated by all monomials $u_{i_0}\cdots u_{i_j}$ of total degree $j + 1$. An element $f \in \mathcal{L}$ can be written in a unique way as a sum $f = \sum f^i$, with $f^i \in \mathcal{L}^i$. Using this grading, the equation $[K, S] = 0$ is equivalent to the set of equations $\sum_i^n [K^i, S^{n-i}] = 0$ for $n = 0, 1, \ldots$. In fact we have here a *bigraded Lie algebra*, where the other grading is just 'the number of derivatives involved', i.e., a term $u_{i_1}\ldots u_{i_r}$ has degree $i_1 + \ldots + i_r$ for this second grading. In the sequel we put this second grading as a subscript. So $u_{i_0}\ldots u_{i_r} \in \mathcal{L}^r_j$ with $j = i_0 + \ldots + i_r$, and $[\mathcal{L}^r_j, \mathcal{L}^s_i] \subset \mathcal{L}^{r+s}_{j+i}$. Note that a nonzero element in $\mathcal{L}^r_i$ is λ-homogeneous of weight $\lambda r + i$.

EXAMPLE 2.4. We fix $\lambda = 2$ and do the Lie-bracket calculation of the symmetry of weight 5 of the λ-homogeneous KdV, using homogeneity and grading. Put $K = u_3 + uu_1$. The symmetry S we try to find, can be written as $S = S^0_5 + S^1_3 + S^2_1$ with $S^j_i \in \mathcal{L}^j_i$. If the linear part S^0_5 of the symmetry is nonzero, me may after rescaling suppose that $S^0_5 = u_5$. It commutes with $K^0_3 = u_3$, hence the $\mathcal{L}^0$-part of $[K, S]$ is indeed 0. Because of homogeneity the quadratic and degree three parts of S can be written as $S^1_3 = a_1u_3u_0 + a_2u_2u_1$ and $S^2_1 = a_3u_1u_0^2$.

The $\mathcal{L}^1$-part of $[K, S]$ then equals

$$[u_3, S^1_3] + [uu_1, S^0_5] = u_5u_1(5 - 3a_1) - 3u_4u_2(a_1 + a_2 - 5) - u_3^2(3a_2 - 10),$$

and this is zero only if $a_1 = \frac{5}{3}$ and $a_2 = \frac{10}{3}$.

Using this, the $\mathcal{L}^2$-part of $[K, S]$ becomes

$$[u_3, S^2_1] + [uu_1, \frac{5}{3}uu_3 + \frac{10}{3}u_1u_2] = (5 - 6a_3)(uu_2^2 + 2u_1^2u_2 + uu_1u_3)$$

which is zero only if $a_3 = \frac{5}{6}$. After having checked that

$$[uu_1, S^2_1] = 0,$$

one may conclude to have found the desired symmetry.

2.3. Symbolic calculus. The 'symbolic method' consists of a rule to translate polynomials in the variables $u = u_0, u_1, u_2, \dots$ into polynomials in the variables u and $\xi_1, \xi_2, \dots$. A first rough approach towards this would be to replace a monomial $u_{i_1} \dots u_{i_r}$ by $\xi_1^{i_1} \dots \xi_r^{i_r} u^r$. However, this is not a good definition, since, for instance, $u_1 u_2 = u_2 u_1$, while $\xi_1 \xi_2^2 u^2 \neq \xi_1^2 \xi_2 u^2$. One makes this well-defined by averaging, i.e., one sends $u_{i_1} \dots u_{i_r}$ to

$$\frac{1}{r!} \sum_\sigma \xi_{\sigma(1)}^{i_1} \dots \xi_{\sigma(r)}^{i_r} u^r,$$

where the summation is over all permutations σ on $\{1, \dots, r\}$. Moreover, one sends 1 to 1 and extends by linearity to obtain a map

$$\mathbb{C}[u, u_1, u_2, \dots] \longrightarrow \mathbb{C}[u, \xi_1, \xi_2, \dots].$$

We use the notation $\widehat{f}$ for the image of f (also called 'the symbolic expression' of f) under this map, and write $f \trianglerighteq \widehat{f}$. This is the *symbolic method*, introduced by Gel'fand and Dikiĭ in [**GD75**], inspired no doubt by classical invariant theory and Fourier transform. The systematic application of it was initiated by Jing Ping Wang in her thesis [**Wan98**].

EXAMPLE 2.5. We repeat the computation of the symmetry of weight 5 for the KdV equation, now using the symbolic method.

The condition in $\mathcal{L}^1$ can be written as $[u_5, uu_1] = [u_3, S_3^1]$. To translate this into symbolic expressions, we use the following.

LEMMA 2.3.1. *If* $f \in \mathcal{L}^1$, *then* $\widehat{[u_n, f]} = (\xi_1 + \xi_2)^n \widehat{f} - (\xi_1^n + \xi_2^n)\widehat{f}$.

Proof. By linearity, it suffices to show this for $f = u_p u_q$. In this case

$$\begin{aligned} [u_n, u_p u_q] &= D_{u_n}(u_p u_q) - D_{u_p u_q}(u_n) \\ &= \textstyle\sum_{j=1}^{n-1} \binom{n}{j} u_{p+j} u_{q+n-j} \\ &\trianglerighteq \tfrac{1}{2} u^2 \textstyle\sum_{j=1}^{n-1} \binom{n}{j} \left(\xi_1^{p+j} \xi_2^{q+n-j} + \xi_1^{q+n-j} \xi_2^{p+j}\right) \\ &= \tfrac{1}{2} u^2 \left(\xi_1^p \xi_2^q + \xi_1^q \xi_2^p\right) \left((\xi_1 + \xi_2)^n - \xi_1^n - \xi_2^n\right). \end{aligned}$$

Since $\widehat{u_p u_q} = \frac{1}{2} u^2 \left(\xi_1^p \xi_2^q + \xi_1^q \xi_2^p\right)$, this proves the lemma. □

For the symbolic expressions corresponding to $[u_5, uu_1] = [u_3, S_3^1]$ this means

$$(\xi_1 + \xi_2)^5 \widehat{uu_1} - (\xi_1^5 + \xi_2^5)\widehat{uu_1} = (\xi_1 + \xi_2)^3 \hat{S}_3^1 - (\xi_1^3 + \xi_2^3)\hat{S}_3^1.$$

We can now (formally) express $\hat{S}^1$ in terms of $\widehat{uu_1}$ as

$$\hat{S}_3^1 = \frac{(\xi_1 + \xi_2)^5 - \xi_1^5 - \xi_2^5}{(\xi_1 + \xi_2)^3 - \xi_1^3 - \xi_2^3} \widehat{uu_1}.$$

This leads to a real solution if $\hat{S}_3^1$ turns out to be a polynomial. Thus our problem gives rise to the following general question, which will be answered in Section 3.1. Let

$$\mathcal{G}_n^1(\xi_1, \xi_2) = (\xi_1 + \xi_2)^n - \xi_1^n - \xi_2^n,$$

then which factors do $\mathcal{G}_n^1$ and $\mathcal{G}_m^1$ have in common?

In our example we have

$$\hat{S}_3^1 = \frac{\mathcal{G}_5^1(\xi_1, \xi_2)}{\mathcal{G}_3^1(\xi_1, \xi_2)} \widehat{uu_1}.$$

Let us introduce ξ_0 by requiring that

$$\xi_0 + \xi_1 + \xi_2 = 0.$$

For odd n, we now have

$$\mathcal{G}_n^1 = -\sum_{i=0}^{2} \xi_i^n,$$

that is, the $\mathcal{G}_n^1$ are S_3-invariants, where S_3 permutes ξ_0, ξ_1, ξ_2. Let

$$c_n = \sum_{i=0}^{2} \xi_i^n, \qquad n = 1, 2, 3.$$

It is known that any S_3-invariant polynomial can be written as $g(c_1, c_2, c_3)$ for some $g \in \mathbb{C}[X, Y, Z]$. Moreover, in our situation $c_1 = 0$, hence the homogeneous $\mathcal{G}_5^1$ must be a multiple of $c_2 c_3$. Comparing coefficients one concludes $\mathcal{G}_5^1 = -\frac{5}{6} c_2 c_3 = \frac{5}{6} c_2 \mathcal{G}_3^1$ and therefore

$$\begin{aligned} \hat{S}_3^1 &= \frac{5}{6} c_2 \widehat{uu_1} \\ &= \frac{5}{6}(\xi_1^3 + 2\xi_1^2 \xi_2 + 2\xi_1 \xi_2^2 + \xi_2^3) u^2. \end{aligned}$$

The unique polynomial in $\mathcal{R}$ with this as symbolic expression is $\frac{5}{3} u u_3 + \frac{10}{3} u_1 u_2$, hence this must be S_3^1.

Next, we compute S_1^2 by solving

$$\widehat{[S_3^1, uu_1]} + \widehat{[S_1^2, u_3]} = 0.$$

This leads to

$$\hat{S}_1^2 = \frac{5}{18}(\xi_1 + \xi_2 + \xi_3) u^3$$

and thus $S_1^2 = \frac{5}{6} u^2 u_1$. Since also $[S_1^2, K_1^1] = 0$, we have found the fifth order symmetry

$$S_5 = S_5^0 + S_3^1 + S_1^2 = u_5 + \frac{5}{3} u u_3 + \frac{10}{3} u_1 u_2 + \frac{5}{6} u^2 u_1.$$

Even though this illustrates the use of the symbolic method on a rather trivial example, already here one can see the simplification it brings and the possibility to apply for instance the invariant theory of the permutation group to attack the classification problem.

The properties of symbolic expressions which were in special cases already used in the above example, are the following.

PROPOSITION 8.

(1) The assignment $f \mapsto \widehat{f}$ is injective. The image of $\mathcal{L}$ under this map consists of all polynomials $g(\xi_1, \dots, \xi_m)u^m$ with $1 \leq m$ and g symmetric.
(2) For $f \in \mathcal{L}^m$ one has $\widehat{D_x(f)} = (\xi_1 + \dots + \xi_{m+1})\widehat{f}$.
(3) For $f \in \mathcal{L}^m$ one has $\widehat{\delta_f(u_n)} = (\xi_1^n + \dots + \xi_{m+1}^n)\widehat{f}$.
(4) For $f \in \mathcal{L}^m$ one has

$$\widehat{[u_n, f]} = \left(\xi_1^n + \dots + \xi_{m+1}^n - (\xi_1 + \dots + \xi_{m+1})^n\right) \widehat{f}.$$

Proof. (2), (3) and (4) follow from straightforward calculations; compare the special case presented as Lemma 2.3.1. To prove (1), first observe that the symbolic expression of a monomial $u_{i_0} \cdots u_{i_m}$ is indeed of the form as stated. Vice versa, every such polynomial $g(\xi_1, \dots, \xi_m)u^m$ is a linear combination of polynomials $(\sum_\sigma \xi_{\sigma(1)}^{i_1} \cdots \xi_{\sigma(m)}^{i_m})u^m/m!$. The latter polynomial is the symbolic expression of $u_{i_1} \cdots u_{i_m}$. This shows both surjectivity and injectivety. □

DEFINITION 2.6. For $n, m \geq 0$, the polynomials $\mathcal{G}_n^m \in \mathbb{Z}[\xi_1, \dots, \xi_{m+1}]$ are defined by $\mathcal{G}_0^m = m$ and

$$\mathcal{G}_n^m = (\xi_1 + \dots + \xi_{m+1})^n - (\xi_1^n + \dots + \xi_{m+1}^n)$$

if $n > 0$.

With these notations, one of the statements in Proposition 8 is that for $f \in \mathcal{L}^m$ and $n \geq 0$ one has $\widehat{[u_n, f]} = \mathcal{G}_n^m \widehat{f}$.

EXAMPLE 2.7. We now turn back to our KdV computation and try to find the quadratic and cubic parts of a λ-homogeneous symmetry of weight $n+2$. We write this symmetry as

$$S = u_{n+2} + S_n^1 + S_{n-2}^2 + \dots.$$

The condition in $\mathcal{L}^1$ is $[u_3, S_n^1] = [u_{n+2}, uu_1]$, hence

$$\hat{S}_n^1 = \frac{\mathcal{G}_{n+2}^1}{\mathcal{G}_3^1}\widehat{uu_1} = \frac{(\xi_1 + \xi_2)^{n+2} - \xi_1^{n+2} - \xi_2^{n+2}}{6\xi_1\xi_2}u^2.$$

This is a polynomial which indeed determines a unique S_n^1. Now consider the cubic term S_{n-2}^2. To solve the equation $[u_3, S_{n-2}^2] + [uu_1, S_n^1] = 0$ corresponding to the $\mathcal{L}^2$-part of $[K, S]$ for S_{n-2}^2, we use the following.

LEMMA 2.3.2. *Suppose* $f, g \in \mathcal{L}^1$ *with* $f \trianglerighteq \widehat{f}$ *and* $g \trianglerighteq \widehat{g}$ *for some* $\widehat{f}, \widehat{g} \in \mathbb{C}[\xi_1, \xi_2]u^2$. *Then the symbolic expression of* $[f, g]$ *equals*

$$\frac{1}{3u}\sum_{\sigma\in S_3} \widehat{f}(\xi_{\sigma(1)}, \xi_{\sigma(2)})\widehat{g}(\xi_{\sigma(3)}, \xi_{\sigma(1)}+\xi_{\sigma(2)}) - \widehat{f}(\xi_{\sigma(1)}, \xi_{\sigma(2)}+\xi_{\sigma(3)})\widehat{g}(\xi_{\sigma(2)}, \xi_{\sigma(3)}).$$

Proof. Both sides of the equality are linear in both f and g, hence it suffices to consider the case $f = u_k u_\ell$ and $g = u_n u_m$. Here a straightforward calculation proves the result (in fact, it is hardly more work to state and prove an analogous result for $f \in \mathcal{L}^r$ and $g \in \mathcal{L}^s$). □

This lemma implies that a solution S_{n-2}^2 exists precisely when

$$\sum_{\sigma\in S_3} \frac{\mathcal{G}_{n+2}^1(\xi_{\sigma(1)} + \xi_{\sigma(2)}, \xi_{\sigma(3)})}{\xi_{\sigma(3)}} - (\xi_{\sigma(1)} + \xi_{\sigma(2)} + \xi_{\sigma(3)})\frac{\mathcal{G}_{n+2}^1(\xi_{\sigma(2)}, \xi_{\sigma(3)})}{\xi_{\sigma(2)}\xi_{\sigma(3)}}$$

is divisible by $\mathcal{G}_3^2 = (\xi_1 + \xi_2 + \xi_3)^3 - \xi_1^3 - \xi_2^3 - \xi_3^3 = 3(\xi_1 + \xi_2)(\xi_2 + \xi_3)(\xi_1 + \xi_3)$. By symmetry, this is the same as divisibility by $(\xi_1 + \xi_2)$. Since the substitution $\xi_2 = -\xi_1$ reduces the above expression to $-2(1 + (-1)^n)\xi_1^{n-1}\xi_3^2$, the desired divisibility holds precisely when n is odd.

In the next section it is shown that no higher degree calculations are needed to prove the existence of infinitely many symmetries for the KdV equation.

2.4. Implicit function theorem. The grading $\mathcal{L} = \oplus_{i=0}^{\infty}\mathcal{L}^i$ induces the structure of a filtered Lie algebra on $\mathcal{L}$. Namely, one puts $\mathcal{F}^i = \oplus_{j\geq i}\mathcal{L}^j$, then $\mathcal{L} = \mathcal{F}^0 \supset \mathcal{F}^1 \supset \mathcal{F}^2 \supset \cdots$ satisfies $\cap_{i=0}^{\infty}\mathcal{F}^i = \{0\}$ and

$$[\mathcal{F}^i, \mathcal{F}^j] \subset \mathcal{F}^{i+j}.$$

In this filtered algebra finding a symmetry S of K is equivalent to solving the set of relations

$$[K, S] \in \mathcal{F}^j \text{ for } j = 1, 2, \ldots$$

Under certain conditions all these relations hold provided the first few do.

DEFINITION 2.8. An element $K \in \mathcal{L}$ is called *nonlinear injective* if $[K, Q] \in \mathcal{F}^{i+1}$ implies $Q \in \mathcal{F}^{i+1}$ for all $Q \in \mathcal{F}^i, i > 0$.

Note that $\mathrm{ad}(K)$ defines a linear map from $\mathcal{F}^i$ to itself, for all i, and hence an induced linear map: $\mathcal{F}^i/\mathcal{F}^{i+1} \to \mathcal{F}^i/\mathcal{F}^{i+1}$ for all i. Nonlinear injective precisely means that these induced maps are injective, for $i > 0$.

Since $[\mathcal{L}^t, \mathcal{F}^i] \subset \mathcal{F}^{t+i}$, nonlinear injectivity of K only depends on the linear part $K^0 \in \mathcal{L}^0$ of K.

DEFINITION 2.9. One calls $K \in \mathcal{L}$ *relative ℓ-prime* with respect to $S \in \mathcal{L}$ if for all $i \geq \ell$ and for all $Q \in \mathcal{F}^i$ one has that $[S, Q] \in \mathrm{ad}(K)(\mathcal{F}^i/)$ implies $Q \in \mathrm{ad}(K)(\mathcal{F}^i) \bmod \mathcal{F}^{i+1}$.

To explain this terminology, note that for $Q \in \mathcal{F}^i$ and $S \in \mathcal{L}$ the class $[S, Q] \bmod \mathcal{F}^{i+1}$ only depends on the Lie bracket $[S^0, Q]$ of Q with the linear part S^0 of S. Similarly, $\mathrm{ad}(K)(\mathcal{F}^i/\mathcal{F}^{i+1}) = \mathrm{ad}(K^0)(\mathcal{F}^i/\mathcal{F}^{i+1})$. Now in the symbolic language, taking the Lie bracket of a linear term $\sum \lambda_j u_j$ and a term $f \in \mathcal{L}^i$ corresponds to multiplying $\widehat{f}$ by $\sum \lambda_j \mathcal{G}_j^i$. If two polynomials g_1, g_2 of this kind are relatively prime in the usual sense, then $g_1 \widehat{f}$ is divisible by g_2 precisely when $\widehat{f}$ is divisible by g_2. Thus, the polynomials being relative prime implies that the corresponding K^0 and S^0 (and hence K and S) are relative ℓ-prime, for all ℓ.

The following implicit function theorem for filtered Lie-algebras, which is to be found in [**SW98**] and in [**Wan98**, Section 2.9], can be used to prove the existence of infinitely many symmetries.

THEOREM 2.10 (Sanders, Wang). *Let $\mathcal{F}$ be a filtered Lie algebra which is complete with respect to the filtration topology. Suppose K, S and $Q \in \mathcal{F}^0$ satisfy*

* $[K, S] = 0$
* *K is nonlinear injective*
* *S is relatively ℓ-prime with respect to K*
* $[K, Q] \in \mathcal{F}^\ell$
* $[S, Q] \in \mathcal{F}^1$.

Then a unique $\tilde{Q} \in \mathcal{F}^\ell$ exists such that $Q + \tilde{Q}$ is a symmetry of both K and S, i.e.,

$$[K, Q + \tilde{Q}] = 0 = [S, Q + \tilde{Q}].$$

The proof of this is actually rather simple: since $[K, S] = 0$ and $[Q, K] \in \mathcal{F}^\ell$, it follows that $[K, [S, Q]] = -[S, [Q, K]] \in \mathcal{F}^\ell$. Nonlinear injectivity of K now implies $[S, Q] \in \mathcal{F}^\ell$. Moreover, the same equality shows that $[S, [K, Q]] \in \mathrm{ad}(K)(\mathcal{F}^\ell/\mathcal{F}^{\ell+1})$. Since S is relatively ℓ-prime with respect to K, it follows that $[K, Q] \equiv [K, Q'] \bmod \mathcal{F}^{\ell+1}$ for some $Q' \in \mathcal{F}^\ell$. Hence $[K, Q - Q'] \in \mathcal{F}^{\ell+1}$ and, using nonlinear injectivity of K as before, also $[S, Q - Q'] \in \mathcal{F}^{\ell+1}$. By induction, the same argument yields for every $p > 0$ an element $Q' \in \mathcal{F}^\ell$ for which $[K, Q - Q']$ and $[S, Q - Q']$ are in $\mathcal{F}^{\ell+p}$. Completeness of $\mathcal{F}$ finishes the argument.

EXAMPLE 2.11. We can now prove that the KdV equation has infinitely many symmetries using this implicit function theorem. So, take $K = u_3 +$

uu_1 and $S = u_5 + \frac{5}{3}uu_3 + \frac{10}{3}u_1u_2 + \frac{5}{6}u^2u_1$. Consider any odd integer n and put $Q = u_{n+2} + S^1_n + S^2_{n-2}$ with S^1_n, S^2_{n-2} as obtained in Example 2.7.

- ∗ We have that $[K, S] = [u_3 + uu_1, u_5 + \frac{5}{3}uu_3 + \frac{10}{3}u_1u_2 + \frac{5}{6}u^2u_1] = 0$.
- ∗ The action of $\mathrm{ad}(K)$ on $\mathcal{F}^i/\mathcal{F}^{i+1}$ equals that of $\mathrm{ad}(u_3)$. This is easily verified to be injective for $i > 0$ (e.g., using the symbolic method).
- ∗ Take $f \in \mathcal{L}^i$. Using the symbolic language one finds that $[S, f] \in \mathrm{ad}(K)(\mathcal{F}^i/\mathcal{F}^{i+1})$ implies $f \in \mathrm{ad}(K)(\mathcal{F}^i/\mathcal{F}^{i+1})$ whenever $\mathcal{G}^i_3$ and $\mathcal{G}^i_5$ are relative prime. It is an easy task to verify that both $\mathcal{G}^3_3$ and $\mathcal{G}^3_5$ are irreducible. Because $\mathcal{G}^i_n|_{(\xi_{i+1}=0)} = \mathcal{G}^{i-1}_n$, all $\mathcal{G}^i_n$ with $n = 3, 5$ and $i > 3$ are irreducible as well. It follows that K is relative 3-prime with respect to S.
- ∗ We have shown in Example 2.7 that $[K, Q] \in \mathcal{F}^3$.
- ∗ Since $[u_5, u_n] = 0$, it follows that $[S, Q] \in \mathcal{F}^1$.

The implicit function theorem therefore yields a Cauchy sequence for the filtration topology $(Q + Q_n)_{n\geq 1}$, with all $Q_n \in \mathcal{F}^3$ and $[K, Q + Q_n]$ and $[S, Q + Q_n]$ elements of $\mathcal{F}^n$. The part of $Q + Q_n$ which is λ-homogeneous of weight $n + 2$ then has be be independent of n for $n >> 0$, and defines a nontrivial symmetry of both K and S. This shows the existence of infinitely many independent symmetries of the KdV equation.

3. Classification results

3.1. Positive weight. Using the symbolic method and the implicit function theorem, the papers [**SW98**] and [**SW00**] classify all λ-homogeneous equations of the form

$$u_t = u_n + f(u_0, \ldots, u_{n-1})$$

which have infinitely many independent symmetries, in the case $\lambda \geq 0$. We briefly indicate the strategy for the case $\lambda > 0$.

Using diophantine approximation theory, F. Beukers [**Beu97**] proved a useful result concerning the mutual divisibility of the G-polynomials:

PROPOSITION 9. *For integers* $m, n, i \geq 1$ *with* $n \neq m$*, the polynomials*

$$\mathcal{G}^i_n = (\xi_1 + \ldots + \xi_{i+1})^n - \xi_1^n - \ldots - \xi_{i+1}^n$$

have the property $\gcd(\mathcal{G}^i_n, \mathcal{G}^i_m) = 1$ *except in the following cases.*

$$\begin{array}{lll} i = 1 & \textit{and } n \textit{ is even}: & \gcd(\mathcal{G}^i_n, \mathcal{G}^i_m) = \xi_1\xi_2 \\ i = 1, & n \equiv 1 \textit{ mod } 6: & \gcd(\mathcal{G}^i_n, \mathcal{G}^i_m) = \xi_1\xi_2(\xi_1+\xi_2)(\xi_1^2+\xi_1\xi_2+\xi_2^2)^2 \\ i = 1, & n \equiv 3 \textit{ mod } 6: & \gcd(\mathcal{G}^i_n, \mathcal{G}^i_m) = \xi_1\xi_2(\xi_1+\xi_2) \\ i = 1, & n \equiv 5 \textit{ mod } 6: & \gcd(\mathcal{G}^i_n, \mathcal{G}^i_m) = \xi_1\xi_2(\xi_1+\xi_2)(\xi_1^2+\xi_1\xi_2+\xi_2^2) \\ i = 2 & \textit{and } n \textit{ is odd}: & \gcd(\mathcal{G}^i_n, \mathcal{G}^i_m) = (\xi_1+\xi_2)(\xi_1+\xi_3)(\xi_2+\xi_3). \end{array}$$

order:	λ:	K:	
$n = 2$	1	$u_2 + u_1 u_0$	(Burgers)
$n = 3$	1	$u_3 + u_1^2$	(potential KdV)
	2	$u_3 + u_1 u_0$	(KdV)
$n = 5$	1	$u_5 + u_1 u_3 + \frac{1}{15} u_1^3$	(potential Sawada-Kotera)
		$u_5 + 10 u_1 u_3 + \frac{15}{2} u_2^2 + \frac{20}{3} u_1^3$	(potential Kaup-Kupershmidt)
		$u_5 + 5 u_1 u_3 + 5 u_2^2 - 5 u_3 u_0^2 - 20 u_2 u_1 u_0 - 5 u_1^3 + 5 u_1 u_0^4$	(Kupershmidt)
$n = 5$	2	$u_5 + 10 u_3 u_0 + 25 u_2 u_1 + 20 u_1 u_0^2$	(Kaup-Kupershmidt)
		$u_5 + 5 u_3 u_0 + 5 u_2 u_1 + 5 u_1 u_0^2$	(Sawada-Kotera)
$n = 3$	$1/2$	$u_3 + 3 u_2 u_0^2 + 9 u_1^2 u_0 + 3 u_1 u_0^4$	(Ibragimov-Shabat)
	1	$u_3 + u_1 u_0^2$	(modified KdV)

TABLE 1. *Integrable λ-homogeneous equations with $\lambda > 0$*

This implies that if a λ-homogeneous equation has no quadratic and no cubic terms, then it cannot have a nontrivial symmetry. Suppose now that the equation K of order n has no quadratic terms. If K has a nontrivial symmetry, then it has a nontrivial λ-homogeneous one. This means in particular that its linear part contains exactly one u_m. Now first of all both n and m have to be odd. We find

$$\widehat{S_m^2} = \frac{\mathcal{G}_m^2}{\mathcal{G}_n^2} \widehat{K_n^2}.$$

In particular, $\widehat{K_n^2}$ is divisible by $\mathcal{G}_n^2 / \left((\xi_1 + \xi_2)(\xi_1 + \xi_3)(\xi_2 + \xi_3) \right)$. Using the implicit function theorem, it follows that K has a λ-homogeneous symmetry of order 3.

If K does have quadratic terms, a similar argument shows that it is in the hierarchy of an equation of order 2,3,5 or 7. A rather extensive computer algebra computation was used to show that if a given 7th order equation has a nontrivial symmetry, then the symbolic expression of its quadratic part is divisible by $(\xi_1^2 + \xi_1 \xi_2 + \xi_2^2)$. This means the equation is in the hierarchy of some fifth order equation. The restriction that the λ-homogeneous equation needs to have a quadratic or a cubic part, reduces the possible values of the weight $\lambda > 0$ to a finite set. Each case has to be checked separately. A system of order $2, 3, 5$ needs to have a symmetry of order $4, 5, 7$, respectively. This results in the list of ten equations in table 3.1.

For the odd order equations in this list which have a quadratic part, one more thing had to be proven. These systems are relative 3-prime while the divisibility results only show that there exists infinitely many symmetries modulo $\mathcal{L}^2$. One proves in this case that $[\widehat{K^1, S^1}]$ is divisible by

$(\xi_1+\xi_2)(\xi_1+\xi_3)(\xi_2+\xi_3)$ if either $\xi_1+\xi_2$ or $\xi_1\xi_2$ divides $\widehat{K^1}$. It follows that the modulo $\mathcal{L}^3$ equation can be solved and using the implicit function theorem once more, this proves the integrability.

3.2. Zero weight. With similar techniques the $\lambda = 0$ case is treated in [**SW00**]. The list is give in table 3.2.

order:	K:	
$n=3$	$u_3+u_1^3$	(potential modified KdV)
$n=5$	$u_5+5u_2u_3-5u^2u_3-5u_1u_2^2+u_1^5$	(potential modified KdV)

TABLE 2. *Integrable λ-homogeneous equations with $\lambda = 0$*

Also noncommutative equations can be considered, in which case u_1u_2 should be read as a tensor product, that is $u_1 \otimes u_2$, and one has to assume there is no relation between $u_1 \otimes u_2$ and $u_2 \otimes u_1$. We omit the results obtained in this case. They can be found in [**OS98, OW00**].

4. Systems of equations

In this survey we will only treat the case of systems of two evolution equations. It should be clear from this what the corresponding notions and definitions in the general case of d equations are.

We take two functions $u = u(x,t)$ and $v = v(x,t)$. As before, the nth derivative with respect to x is denoted u_n and v_n, respectively. By u_t and v_t one denotes the derivative with respect to t. The equations considered have the form

$$\begin{cases} u_t = K(u,u_1,\ldots,v,v_1,\ldots) \\ v_t = L(u,u_1,\ldots,v,v_1,\ldots) \end{cases}$$

in which K, L are functions of u and v and of finitely many of their derivatives u_i, v_j. The maximal n such that u_n or v_n appears in one of K, L is called the *order* of the equation, or of K, L. The *dimension* of the equation is the number of functions involved, which is 2 in our case.

4.1. Symmetries. The vector $S(u,u_1,\ldots,v,v_1,\ldots))$ is a *symmetry* of the equation if

$$\begin{cases} \frac{d}{dt}(u+S_1) = K(u+\varepsilon S_1, u_1+\varepsilon D_x(S_1),\ldots, v+\varepsilon S_2, v_1+\varepsilon D_x(S_2),\ldots) \\ \frac{d}{dt}(v+S_2) = L(u+\varepsilon S_1, u_1+\varepsilon D_x(S_1),\ldots, v+\varepsilon S_2, v_1+\varepsilon D_x(S_2),\ldots) \end{cases}$$

upto first order in ε. Analogous to the case of scalar equations, one obtains an algebraic description (limited to polynomial equations) as follows.

Write $\mathcal{R} := \mathbb{C}[u,u_1,\ldots,v,v_1,\ldots]$ for the ring of polynomials over $\mathbb{C}$ in infinitely many variables $u = u_0, u_1, \ldots, v = v_0, v_1, \ldots$. One fixes a $\mathbb{C}$-linear derivation δ_x on $\mathcal{R}$ defined by $\delta_x(u_i) = u_{i+1}$ and $\delta_x(v_i) = v_{i+1}$. For any pair $(f, g) \in \mathcal{R} \times \mathcal{R}$ there is a unique $\mathbb{C}$-linear derivation on $\mathcal{R}$, denoted by $\delta_{(f,g)}$, satisfying $\delta_{(f,g)}(u) = f$ and $\delta_{(f,g)}(v) = g$. Note that $\delta_{(f,g)}(h)$ is in fact the *Fréchet derivative* of h in the direction (f, g), c.f. [**Olv93**, 5.24], also called the *Gateaux derivative* ([**Mag78**, A1]). One extends such a derivation to the ring of dual numbers $\mathcal{R}[\varepsilon]$ by $\delta_{(f,g)}(r + \varepsilon s) = \delta_{(f,g)}(r) + \varepsilon\delta_{(f,g)}(s)$.

With these notations, $S = (S_1, S_2) \in \mathcal{R} \times \mathcal{R}$ is a symmetry of $K = (K_1, K_2) \in \mathcal{R} \times \mathcal{R}$ precisely when

$$\begin{cases}\delta_K(u + \varepsilon S_1) = K_1(u + \varepsilon S_1, u_1 + \varepsilon\delta_x(S_1), .., v + \varepsilon S_2, v_1 + \varepsilon\delta_x(S_2), \ldots)\\ \delta_K(v + \varepsilon S_2) = K_2(u + \varepsilon S_1, u_1 + \varepsilon\delta_x(S_1), .., v + \varepsilon S_2, v_1 + \varepsilon\delta_x(S_2), \ldots).\end{cases}$$

Completely analogous to the scalar case, one calculates that this is equivalent to the vanishing of a Lie bracket $[K, S]$ on $\mathcal{R} \times \mathcal{R}$, defined by

$$[K, S] := (\delta_K(S_1) - \delta_S(K_1), \delta_K(S_2) - \delta_S(K_2)).$$

The symmetries of K form a sub-Lie-algebra of $\mathcal{R} \times \mathcal{R}$. The $\mathbb{C}$-linear combinations of (u_1, v_1) and (K_1, K_2) are contained in this; they are called *trivial* symmetries. The system K is called *integrable* if this sub-Lie-algebra has infinite dimension over $\mathbb{C}$.

4.2. Homogenuity and grading. As in the scalar case, write $\mathcal{L}$ for the subspace of $\mathcal{R}$ consisting of all polynomials with constant term 0. Given integers $r, s, n \geq 0$, the linear subspace $\mathcal{L}_n^{r,s}$ is by definition the $\mathbb{C}$-span of all monomials $u_{i_0} \cdots u_{i_r} v_{j_0} \cdots v_{j_s}$ with $i_0 + \ldots + i_r + j_0 + \ldots + j_s = n$. This defines three gradings on $\mathcal{L}$, and $\mathcal{L} = \oplus_{r,s,n} \mathcal{L}_n^{r,s}$.

Given real numbers (λ_1, λ_2) and w, a pair $(K, L) \in \mathcal{L} \times \mathcal{L}$ is called (λ_1, λ_2)*-homogeneous of weight* w if all $\mathcal{L}_n^{r,s}$-parts of K satisfy $r\lambda_1 + s\lambda_2 + n = w + \lambda_1$ and all $\mathcal{L}_n^{r,s}$-parts of L satisfy $r\lambda_1 + s\lambda_2 + n = w + \lambda_2$.

Note that the linear parts of a homogeneous pair are of the form $(au_n + bv_n, cu_n + dv_n)$. Moreover, if both $\lambda_1, \lambda_2 > 0$ then the number n appearing here is larger than the order of the higher degree parts of K and L. We will restrict ourselves to (λ_1, λ_2)-homogeneous systems $(K, L) \in \mathcal{L} \times \mathcal{L}$ with $\lambda_1, \lambda_2 > 0$ which moreover have the property that the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ can be diagonalized. If this is the case, a linear transformation changes the pair into one of the form $(a_1 u_n + K', a_2 v_n + L')$ with K', L' of order $< n$. The values a_1, a_2 are called the *eigenvalues* of the system. For such systems we will show that a nontrivial condition for integrability can be analyzed using divisibility properties of the $\mathcal{G}$-functions introduced in the next section.

4.3. Symbolic method. In the 2-dimensional case, the *symbolic expression* of $f \in \mathcal{L}$ is by definition its image $\widehat{f}$ in the ring of polynomials

$\mathbb{C}[u, v, \xi_1, \xi_2, \ldots, \eta_1, \eta_2, \ldots]$ under the $\mathbb{C}$-linear map defined by

$$u_{i_1} \cdots u_{i_r} \cdot v_{j_1} \cdots v_{j_s} \mapsto u^r v^s \frac{1}{r!s!} \sum_{\sigma \in S_r, \tau \in S_s} \xi_{\sigma(1)}^{i_1} \cdots \xi_{\sigma(r)}^{i_r} \eta_{\tau(1)}^{j_1} \cdots \eta_{\tau(s)}^{j_s}.$$

The properties of this assignment are analogous to those for the scalar case: if $f \in \mathcal{L}^{r,s}$, then

$$\widehat{D_x f} = (\sum_{i=1}^{r+1} \xi_i + \sum_{j=1}^{s+1} \eta_j) \widehat{f}.$$

For $f, g \in \mathcal{L}^{i,j}$, the bracket $[(a_1 u_n, a_2 v_n), (f, g)]$ corresponds in the symbolic language to multiplication of $(\widehat{f}, \widehat{g})$ with the diagonal matrix

$$\begin{pmatrix} G_{u;n}^{i,j}[a] & 0 \\ 0 & G_{v;n}^{i,j}[a] \end{pmatrix}$$

where

$$G_{u;n}^{i,j}[a] = a_1 (\sum_{k=1}^{i+1} \xi_k + \sum_{l=1}^{j} \eta_l)^n - a_1 \sum_{k=1}^{i+1} \xi_k^n - a_2 \sum_{l=1}^{j} \eta_l^n$$

and

$$G_{v;n}^{i,j}[a] = a_2 (\sum_{k=1}^{i} \xi_k + \sum_{l=1}^{j+1} \eta_l)^n - a_1 \sum_{k=1}^{i} \xi_k^n - a_2 \sum_{l=1}^{j+1} \eta_l^n,$$

which are related by

$$G_{u;n}^{i,j}[a_1, a_2](\xi, \eta) = G_{v;n}^{j,i}[a_2, a_1](\eta, \xi).$$

4.4. Example: a degenerate integrable system. In this section we demonstrate the use of the symbolic method and the implicit function theorem by proving the integrability of some degenerate system consisting of the KdV equation coupled to a purely non-linear equation with a parameter.

Start with the following system, to be found in [**Fou00**]:

$$\begin{cases} u_t = \frac{1}{2} u_3 + \frac{1}{2} v_3 + (2-\alpha) u_0 u_1 + (6-\alpha) v_0 u_1 + \alpha u_0 v_1 + (4-\alpha) v_0 v_1 \\ v_t = \frac{1}{2} v_3 + \frac{1}{2} u_3 + (2-\alpha) v_0 v_1 + (6-\alpha) u_0 v_1 + \alpha v_0 u_1 + (4-\alpha) u_0 u_1. \end{cases}$$

Using the invertible linear transformation

$$u \mapsto \frac{1}{2}(u+v), v \mapsto \frac{1}{2}(u-v)$$

and applying the scale transformation $u \mapsto \frac{1}{2} u$ and the parameter translation $\alpha \mapsto \alpha + 2$, this is transformed into the system

$$K(\alpha) := \begin{cases} u_t &= u_3 + 3 u_0 u_1 \\ v_t &= \alpha u_1 v_0 + u_0 v_1. \end{cases}$$

This system has infinitely many symmetries for any α, as is shown as follows. Write K_n (with n odd) for the nth order symmetry in $\mathbb{C}[u, u_1, \ldots, u_n]$ of the KdV equation. It follows from [**Olv93**, 5.31] that every K_n is the D_x-image of a unique element in $\mathbb{C}[u, u_1, \ldots, u_n] \cap \mathcal{L}$; this element is denoted $D_x^{-1}(K_n)$. As is shown in *loc. cit.*, they satisfy the recursive relation $K_{n+2} = D_x^2(K_n) + 2uK_n + u_1 D_x^{-1}(K_n)$. A direct calculation now shows that for every odd $n \geq 3$, the pair

$$S_n(\alpha) = \begin{pmatrix} K_n \\ (\alpha v_0 + v_1 D_x^{-1}) K_{n-2} \end{pmatrix}$$

is a symmetry of the system $K(\alpha)$. Hence this system is integrable.

In fact, much more can be proven: by taking these $S_n(\alpha)$ and $K(\alpha)$ as input in the implicit function theorem, it was shown in [**vdK02**] (using the symbolic method) that $K(\alpha)$ also has symmetries of every even order (at least for $\alpha \neq 2$). As a special case, this proves a conjecture of Foursov [**Fou00**]).

5. Classification results

As in the scalar case, to use the symbolic method in order to classify integrable homogeneous systems one needs divisibility results for $\mathcal{G}$-polynomials. In the present situation, these (homogeneous) polynomials depend on integers $n, m > 0$ and a vector $\underline{a} = (a_0, \ldots, a_m) \in \mathbb{C}^{m+1}$; they are denoted $\mathcal{G}_n^m[\underline{a}]$, with

$$\mathcal{G}_n^m[\underline{a}] := a_0 \left(\xi_1 + \ldots + \xi_m\right)^n - a_1 \xi_1^n - \ldots - a_m \xi_m^n.$$

5.1. Systems without quadratic and cubic terms. The following theorem implies that any polynomial (in $u, v, \cdots$ and their x-derivatives) system of order $n > 1$ with nonzero diagonal linear part and without quadratic and cubic terms cannot have higher order nontrivial symmetries.

THEOREM 5.1. *Let* $3 < n \in \mathbb{N}$*. For any positive integer* m *and vector* $\underline{a} = (1, a_1^{m-1}, \ldots, a_n^{m-1})$*, the* $\mathcal{G}$*-function*

$$g_{a,m} = \mathcal{G}_m^n[\underline{a}] = (\sum_{i=1}^{n} \xi_i)^m - \sum_{i=1}^{n} a_i^{m-1} \xi_i^m$$

is irreducible over $\mathbb{C}$ *in case all* $a_i \neq 0$*.*

PROOF. A factorization $f_{a,m} = A \cdot B$ with A, B polynomials of positive degree, means that the projective hypersurface S given by $f_{a,m} = 0$ is a union of two components S_1 and S_2. Since $n > 3$, these components intersect in an infinite number of points, which should be singularities of S. A straightforward calculation shows that S has only finitely many singular points. Hence $f_{a,m}$ is irreducible. □

5.2. Cubic terms. Suppose that our integrable two-dimensional system has nonzero cubic part $K^{-1,2}$ or $K^{2,-1}$. The following theorem implies that all its eigenvalues are equal and its order is 3.

THEOREM 5.2. *Let $a \in \mathbb{C}$ and $n \in \mathbb{Z}_{>1}$. Consider the polynomial*

$$f_{a,n} = a(x+y+z)^n - x^n - y^n - z^n$$

If $a = 1$ and n odd we have

$$f_{1,n} = (x+y)(y+z)(x+z)F_n(x,y,z)$$

with $F_n(x,y,z)$ irreducible in $\mathbb{C}[x,y,z]$.

If $n = 2$ and $a = 1/3$ then $f_{1/3,2} = -\frac{2}{3}(x+\rho y+\bar{\rho}z)(x+\bar{\rho}y+\rho z)$ in which $\rho = e^{2\pi i/3}$.

In all other cases $f_{a,n}$ is irreducible in $\mathbb{C}[x,y,z]$.

The idea of the proof is to show that the number of singularities on the curve given by $f_{a,n} = 0$ is too small for the curve to be reducible. This was actually carried out by Frits Beukers.

Other progress can be made under the assumption that the order of the equation is two. This is carried out in [**SW01**]. With help of Taylor's expansion it is possible to show the following.

THEOREM 5.3. *Suppose $\underline{a}, \underline{b} \in \mathbb{P}^3(\mathbb{C})$ have the property that there exists more than value $m \in \mathbb{N}$ such that $\mathcal{G}_2^3[\underline{a}]$ divides $\mathcal{G}_m^3[\underline{b}]$. Then all such m have the same parity and we are in one of the following cases:*

(1) $\underline{a} = (1,1,1,-1)$ *and* $\underline{b} = (1,1,1,\pm 1)$.
(2) $\underline{a} = (1,1,-1,1)$ *and* $\underline{b} = (1,1,\pm 1,1)$.

With these two theorems and the implicit function theorem we can draw the following conclusions:

* Under the usual assumptions, if the 2^{nd}-order system without quadratic terms is integrable, then its only eigenvalue is -1 and it has arbitrary order symmetries.
* This analysis is also useful in dimension $d > 2$. However, only for $d = 2$ it gives a complete answer: we only have two eigenvalues, so either a_1, a_2 or a_3 is equal to a_0, or they are all different from a_0 and therefore equal to one another.
* Although we only consider the integrability problem, the results equally apply to almost integrable systems (that is, systems with only a finite number of nontrivial generalized symmetries).

There is still a lot to be done here. The mutual divisibility of the polynomials

$$\mathcal{G}_n^3[\underline{v}] = a(x+y+z)^n - bx^n - cy^n - dz^n$$

(with $\underline{v} = (a, b, c, d)$) is well understood for $b = c = d$ and we know when the quadratic one appears as a factor of an other one, but that is it. Progress here would have immediate implications in the classification theory of systems of evolution equations with respect to the existence of symmetries.

5.3. Quadratic terms. We proceed as in the previous subsection. First we assume that our two dimensional system has nonzero part $K^{-1,1}$ or $K^{1,-1}$. Number theoretical methods and 'experimental mathematics' will lead us to many integrable systems at any order. Moreover we will find a huge set of almost integrable systems, that is to say systems with a finite number of symmetries. It was observed and conjectured, cf. [**Fok80, IŠ80, Fok87**], that the existence of one (or a few) symmetries implies the existence of infinitely many symmetries. This turns out to be wrong. Counterexamples were found in [**Bak91, vdKS99**]. A (p-adic) method to prove that the number of symmetries is finite has been developed, cf. [**BSW98, vdKS01**]. We will first concentrate on integrable systems. After this, we indicate how the p-adic methods work. Finally, we fix the order and show how to classify the general system of order two using number theory.

5.3.1. *Integrable $\mathcal{B}$-systems.* Suppose that $K^{-1,1}$ is non-zero. The system contains the following subsystem which we will analyze on its own.

$$\mathcal{B}_n[a_1, a_2](K) : \begin{cases} u_t = & a_1 u_n + K(v_0, v_1, \ldots) \\ v_t = & a_2 v_n \end{cases}$$

where $a_1, a_2 \in \mathbb{C}$ and K is a quadratic polynomial in $v_0, v_1, v_2, \ldots$. We call this a $\mathcal{B}$–system. The (only) condition for $\mathcal{B}_m[b_1, b_2](S)$ to be a symmetry of $\mathcal{B}_n[a_1, a_2](K)$ reads

$$G_n[a_1, a_2]\widehat{S} = G_m[b_1, b_2]\widehat{K},$$

with the G–functions

$$G_n[a_1, a_2](\xi_1, \xi_2) = a_1(\xi_1 + \xi_2)^n - a_2(\xi_1^n + \xi_2^n).$$

If $G_m[b_1, b_2]\widehat{K}$ is divisible by $G_n[a_1, a_2]$ we have a symmetric polynomial expression for $\widehat{S}$ which can be transformed back. Because the ξ_1-degree of $\widehat{K}$ is assumed to be smaller than n, the function $G_n[a_1, a_2]$ cannot divide $\widehat{K}$. Therefore $G_n[a_1, a_2]$ should have a common factor with $G_m[b_1, b_2]$ in case a nontrivial symmetry (with eigenvalues b_1, b_2) exists. Vice versa, if $a_1, a_2, b_1, b_2 \in \mathbb{C}$ satisfy (with $F, L, T \in \mathbb{C}[\xi_1, \xi_2]$)

$$\begin{aligned} G_n[a_1, a_2] &= FL \\ G_m[b_1, b_2] &= FT \end{aligned}$$

with F not constant, then the Lie bracket vanishes if one takes K, S corresponding to multiples LM and MT. One is free to choose $M \in \mathbb{C}[\xi_1, \xi_2]$ as long as the ξ_1-degree of K is smaller than n.

THEOREM 5.4. *All first, second and third order $\mathcal{B}$-systems are integrable.*

PROOF. The $\mathcal{G}$-functions of these systems are symmetric binary forms of degree 1 or 2. The only one of degree 1 is $\xi_1+\xi_2$, which divides $G_m[b_1, b_2]$ if and only if m is odd. A second degree symmetric form has two zeroes r and $\frac{1}{r}$. It divides $G_m[1 + r^m, (1 + r)^m]$ for every m. □

This also shows that to obtain higher order integrable systems that are not in the hierarchy of a lower order system, one has to consider factors of degree 4.

LEMMA 5.3.1. *Suppose $r \neq s$. The form $G_n[1 + r^n, (1 + r)^n]$ has a factor*

$$(\xi_1 - r\xi_2)(r\xi_1 - \xi_2)(\xi_1 - s\xi_2)(s\xi_1 - \xi_2)$$

whenever

$$U_n(r, s) := G_n[1 + r^n, (1 + r)^n](1, s) = 0.$$

PROOF. This is evident by comparing zeroes. □

To find integrable $\mathcal{B}$-systems that are not in a hierarchy of a system of order smaller than 4, one needs r, s such that $U_m(r, s) = 0$ for infinitely many positive m. Since $U_m(r, s) = (1 + s)^m + (r + rs)^m - (1 + r)^m - (s + rs)^m$, the following theorem can be applied.

THEOREM 5.5 (Lech, Mahler). *Let $x_1, x_2, \ldots, x_k, c_1, c_2, \ldots, c_k \in \mathbb{C}\backslash 0$. Suppose that none of the ratios x_i/x_j with $i \neq j$ is a root of unity. Then the equality*

$$c_1x_1^m + c_2x_2^m + \ldots + c_kx_k^m = 0$$

holds for at most finitely many integers m.

In [**BSW98**] it is shown that as a consequence of this, the only factors of G–functions (with a nonzero a_i) which appear in infinitely many other ones G_m, have zeroes in a set of the form $\{0, -1, r, \frac{1}{r}, \bar{r}, \frac{1}{\bar{r}}\}$. The following list of all integrable $\mathcal{B}$–systems with quadratic part v_0^2 given in [**BSW01**] is obtained using this. It also used an algorithm of C.J. Smyth (cf [**BS01**]) that solves polynomial equations for roots of unity. For each system in the list, all n such that a (nontrivial) symmetry $\mathcal{B}_n$ exists, are given.

$$n \in \mathbb{N} \quad \begin{cases} au_2 + v^2 \\ v_2 \end{cases} \qquad n \in 2\mathbb{N}+1 \quad \begin{cases} au_3 + v^2 \\ v_3 \end{cases}$$

$$n \in 3\mathbb{N}+1 \quad \begin{cases} -u_4 + v^2 \\ v_4 \end{cases} \qquad n \in 4\mathbb{N} \quad \begin{cases} -3u_4 + v^2 \\ v_4 \end{cases}$$

$$n \in 4\mathbb{N}+1 \quad \begin{cases} -\frac{1}{4}u_5 + v^2 \\ v_5 \end{cases} \qquad n \in 10\mathbb{N}+5 \quad \begin{cases} \frac{-13\pm5\sqrt{5}}{2}u_5 + v^2 \\ v_5 \end{cases}$$

$$n \in 6\mathbb{N}\pm1 \quad \begin{cases} u_5 + v^2 \\ v_5 \end{cases} \qquad n \in 6\mathbb{N}+1 \quad \begin{cases} u_7 + v^2 \\ v_7 \end{cases}$$

We now present a more direct method than the one in [**BSW01**]. This makes it possible to treat higher orders. Expressing $U_n(r, \bar{r})$ in terms of $x = \frac{r}{\bar{r}}$ and $y = \frac{1+r}{1+\bar{r}}$ yields an equation that can be solved for roots of unity. As an example, this was carried out for $n \leq 23$, and the values r corresponding to solutions x, y were plotted. Because the set of roots is invariant under $r \mapsto \frac{1}{r}$ and $r \mapsto \bar{r}$, the upper half unit disc is taken as a fundamental domain. Inspecting the patterns formed by the values r obtained in this way, can be described as *experimental mathematics*.

To explain the results which were at first found experimentally in this way, note that any $r \in \mathbb{C} \setminus \mathbb{R}$ can be described by fixing two unit vectors ψ, φ in the upper half plane and saying that r is the intersection of the lines $a\psi$ and $-1 + b\varphi$.

THEOREM 5.6. *Let $3 < n \in \mathbb{N}$. Let ψ, φ be $2n^{th}$ roots of unity. Let $\mathcal{H} = \{z \in C | z \neq \bar{z}, |z| \neq 1\}$. To the intersection point $r \in \mathcal{H}$ of the lines $a\psi$ and $-1 + b\varphi$, there corresponds an integrable $\mathcal{B}$-system.*

Any integrable $\mathcal{B}$-system is a symmetry of such a system.

The proof of the first statement is simple, it follows from substituting r in $U_m(r, \bar{r})$. The ratio of eigenvalues of the integrable $\mathcal{B}$-system is given by $(1 + r^n)/(1 + r)^n$ and the order of the symmetries is a multiple of n. The second statement follows from the Lech-Mahler theorem.

The number of integrable systems of this form can be calculated and it can be verified whether such a system is in a lower hierarchy.

THEOREM 5.7. *Let $\mathcal{K} = \{z \in \mathcal{H} | z + \bar{z} \neq -2, |z + \frac{1}{2}| \neq \frac{1}{2}\}$. The $\mathcal{B}$-systems described in theorem 5.6 that correspond to $r \in \mathcal{K}$ have no other symmetries.*

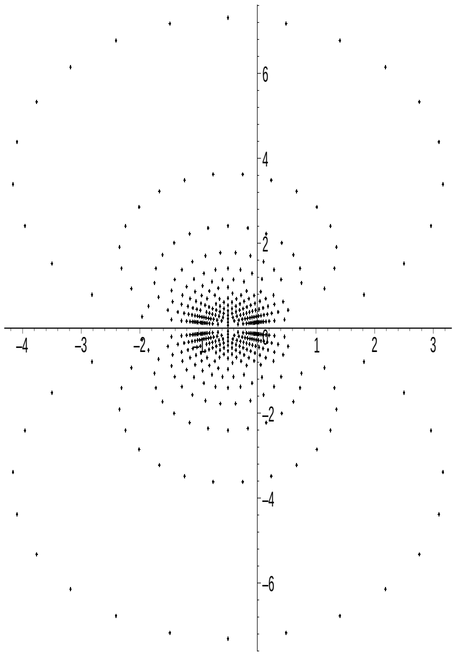

FIGURE 1. *The pattern of zeroes of G–polynomials of integrable systems with order* 23.

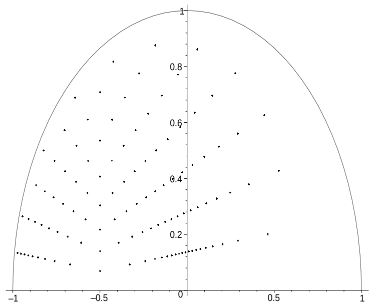

FIGURE 2. *The zeroes of G–polynomials of integrable systems with order* 10 *inside the unit disc as intersections of stars.*

The idea of the proof is, to write $U_m(r, \bar{r})$ in terms of roots of unity ψ and φ and to perform the transformation

$$\varphi^2 \to \nu, \ \psi^2 \to \mu\nu.$$

This leads to the diophantine equation

$$\left(\frac{1-\mu}{1-\nu}\right)^m = \frac{1-\mu^m}{1-\nu^m} \tag{5.1}$$

Frits Beukers showed that when $m > 1$, this equation has no solutions in roots of unity μ, ν with $\mu, \nu \neq \pm 1$ and $\mu \neq \nu, \bar{\nu}$. Applying the inverse transformation to $\mu, \nu = -1$ results in $\varphi = \pm i\psi, \varphi = \pm 1$.

One may observe that the remaining integrable $\mathcal{B}$-systems do not have other symmetries as well. To show this, one proves that the diophantine equation

$$(1+\mu)^n = 2^{n-1}(1+\mu^n)$$

has no solutions with $n > 1$ and μ a root of unity $\neq \pm 1$. This follows by comparing a 2-adic valuation of the two sides. This observation in fact completes the classification of integrable $\mathcal{B}$-systems.

EXAMPLE 5.8. Take $n = 6$. The line $\alpha e^{\frac{1}{3}\pi i} - 1$ intersects the imaginary axis in the point $r = \sqrt{3}i$. This is a zero of $G_6[13, -32]$. The polynomial dividing all G–functions of the corresponding symmetries is

$$Q = (3\xi_1^2 + \xi_2^2)(\xi_1^2 + 3\xi_1^2)$$

The quadratic part of the system yields (a multiple of)

$$\frac{G_6[13, -32]}{2Q} = \frac{15}{2}(\xi_1^2 + \xi_2^2) + 13\xi_1\xi_2.$$

One easily calculates using this, that the system

$$\begin{cases} u_t = & 13u_6 + 15vv_2 + 13v_1^2 \\ v_t = & -32v_6 \end{cases}$$

has a symmetry

$$\begin{cases} 365u_{12} - 561vv_8 + 1460v_1v_7 + 9900v_2v_6 + 21900v_3v_5 + 13893v_4^2 \\ 2048v_{12} \end{cases}$$

5.3.2. *Almost integrable $\mathcal{B}$-systems.* Many $\mathcal{B}$-systems have only finitely many independent symmetries. An efficient method for computing all $\mathcal{B}$-systems of a given order with a symmetry of some other fixed order is the use of resultants.

We fix integers $n \neq m$ and calculate all r, s (with $r \neq s, \frac{1}{s}$) such that $U_n(r, s) = U_m(r, s) = 0$. In the following we disregard the trivial factors of U_n which are $(r-s)(rs-1)$ for all n and also $(r+1)(s+1)$ for odd n.

LEMMA 5.3.2. *Take $n > 3$. To obtain all eigenvalues of n^{th} order $\mathcal{B}$-systems with a symmetry of order $m \neq n$ one calculates the resultant of $U_n(r, s)$ and $U_m(r, s)$ with respect to s and applies the map $r \mapsto \frac{1+r^m}{(1+r)^m}$ to its zeroes.*

PROOF. If the resultant of $U_n(r, s)$ and $U_m(r, s)$ vanishes for some number $r \in \mathbb{C}$ then by lemma 5.3.1, the two symmetric binary forms $G_n[1 + r^n, (1+r)^n](\xi_1, \xi_2)$ and $G_m[1+r^m, (1+r)^m](\xi_1, \xi_2)$ have a common fourth order factor Q. This implies that the n^{th} order $\mathcal{B}$–system with eigenvalues $a_1 = 1+r^n, a_2 = (1+r)^n$ and quadratic part corresponding to $G_n[a_1, a_2]/Q$ has a symmetry of order m. ☐

EXAMPLE 5.9 (Bakirov, [**Bak91**]). The resultant of U_4 and U_6 with respect to s contains the factor

$$f(r) = 2r^4 + 10r^3 + 15r^2 + 10r + 2.$$

We have that

$$1 + r^4 \equiv 5(1 + r)^4 \bmod f(r)$$

and

$$1 + r^6 \equiv 11(1 + r)^6 \bmod f(r).$$

Hence a 4th order system with eigenvalues 5 and 1 has a 6th order symmetry with eigenvalues 11 and 1.

To obtain an explicit example, take $K = v^2$. Then the quadratic part of the 6th order symmetry satisfies

$$\widehat{S^1} = \frac{G_6[11,1](\xi_1,\xi_2)}{G_4[5,1](\xi_1,\xi_2)} v^2 = (5\frac{\xi_1^2 + \xi_2^2}{2} + 4\xi_1\xi_2)v^2,$$

hence $S^1 = 5v_0v_2 + 4v_1^2$. Thus we have calculated that

$$\begin{cases} u_t = & 5u_4 + v_0^2 \\ v_t = & v_4 \end{cases}$$

has the sixth order symmetry

$$\begin{cases} u_t = & 11u_6 + 5v_0v_2 + 4v_1^2 \\ v_t = & v_6 \end{cases}$$

We will now discuss p-adic techniques to answer the question, whether a particular system has more than one independent symmetry, and if so, of what order. In fact, the method will enable us to show that a system has only finitely many generalized symmetries.

Let p be a prime number. The ring of p-adic integers is denoted by $\mathbb{Z}_p$ and its field of fractions by $\mathbb{Q}_p$. The ring of p-adic integers is $\mathbb{Z}_p$. An introductory text on p-adic numbers is provided by [**Gou97**]. Every element $x \in \mathbb{Z}_p$ can be written as

$$x = \sum_{i=0}^{\infty} c_i p^i$$

with $c_i \in \{0, 1, \ldots, p-1\}$ and this representation is unique. The p-adic expansion of a positive integer is just its base p representation, and this yields inclusions $\mathbb{Z} \subset \mathbb{Z}_p$ and $\mathbb{Q} \subset \mathbb{Q}_p$. We have (compatible) reductions modulo p^n given by $\sum_{i=0}^{\infty} c_i p^i \mapsto \sum_{i=0}^{n-1} c_i p^i \bmod p^n$.

Hensel lifting. Hensel's lemma gives a method to check whether a polynomial over $\mathbb{Z}_p$ has a zero in $\mathbb{Z}_p$:

LEMMA 5.3.3 (Hensel). *A polynomial $f \in \mathbb{Z}_p[X]$ has a zero in $\mathbb{Z}_p$, provided the following holds. There exists an $\alpha_1 \in \mathbb{Z}_p$ such that $f(\alpha_1) \equiv 0 \bmod p$ and $\frac{df}{dr}(\alpha_1) \not\equiv 0 \bmod p$.*

The (standard) proof is to construct a Cauchy sequence in $\mathbb{Z}_p$ using Newton iteration, starting from α_1.

The method of Skolem. Let j be a positive integer. Given p-adic integers c_i and p-adic units x_i for $1 \leq i \leq j$, one puts

$$u_n^m = \sum_{i=1}^{j} c_i y_i^m x_i^n$$

where $y_i \in \mathbb{Z}_p$ is defined by $1 + py_i = x_i^{p-1}$. For example, with $c_i = (-1)^i$ and $j = 4$ and $x_1 = 1 + r$, $x_2 = 1 + s$, $x_3 = s + rs$ and $x_4 = r + rs$ we have $U_n(r, s) = u_n^0$.

LEMMA 5.3.4 (Skolem). *If $u_k^0 \not\equiv 0$ mod p then $\forall r \; u_{k+r(p-1)}^0 \neq 0$.*

PROOF. Note that $u_{k+r(p-1)}^0 = \sum_{i=1}^{j} c_i x_i^k (1 + y_i p)^r \equiv u_k^0 \bmod p$. □

LEMMA 5.3.5 (Skolem). *If $p > 2$ and $u_k^0 = 0$ and $u_k^1 \not\equiv 0$ mod p then $\forall r > 0$ we have $u_{k+r(p-1)}^0 \neq 0$.*

PROOF. Assume $u_{k+r(p-1)}^0 = 0$, then

$$0 = \sum_{i=1}^{j} c_i x_i^k (1 + y_i p)^r = \sum_{t=0}^{r} \binom{r}{t} p^t u_k^t = \sum_{t=1}^{r} \binom{r}{t} p^t u_k^t.$$

Now use

$$\frac{1}{r}\binom{r}{t} = \frac{1}{t}\binom{r-1}{t-1}$$

and divide by pr to obtain

$$u_k^1 + \sum_{t=2}^{r} \binom{r-1}{t-1} \frac{p^{t-1}}{t} u_k^t = 0.$$

This contradicts the second assumption since $\frac{p^{t-1}}{t}$ contains a factor p for $t \geq 2$ and $p \neq 2$. □

To apply these lemmas in our situation, recall that we are have a pair $n \neq m$ and a solution r, s to the system $U_m(r,s) = U_n(r,s) = 0$. We want to find conditions on other integers k such that $U_k(r,s) = 0$. For this, one searches a prime number p such that the involved roots r and s are in $\mathbb{Z}_p$, and one considers the corresponding u_k^0 (with $j = 4$). One now checks the conditions in the lemmas for all $k < p - 1$.

EXAMPLE 5.10. Here is how to apply the method of Skolem to the Bakirov system. Recall that the resultant of U_4 and U_6 contains a quartic polynomial $f(r) = 2r^4 + 10r^3 + 15r^2 + 10r + 2$.

* When $p = 23$ we find modulo p the simple zeroes 7 and 10. These are each others inverse so there is a (23-adic) G–function containing them at every order. Hence no additional condition on the order of possible symmetries is found here.
* At $p = 59$ we find modulo p simple zeroes $25, 26, 27, 35$ from which we choose 25 and 27. By Hensel's lemma, they correspond to p-adic zeroes $r := 25 + 37 \cdot 59 + \ldots$ and $s := 27 + 26 \cdot 59 + \ldots$ of f.

  The expression $u_m^0 = U_m(r,s)$ vanishes modulo p when $m \in \{0, 1, 4, 6, 29, 30, 33, 35\}$ and is non-zero for other $m < 58$. This in fact implies that there is no other symmetry of order less than 58. With the first lemma of Skolem one concludes that any symmetry has order $\equiv m \bmod 59$ with $m \in \{0, 1, 4, 6, 29, 30, 33, 35\}$.

  However, $u_m^0 \not\equiv 0 \bmod p^2$ when $m \in \{29, 30, 33, 35\}$. Therefore we can not apply the second lemma in these cases.
* In $\mathbb{Z}_{181}$ we find the zeroes $r = 66 + 13p + \ldots$ and $s = 139 + 29p + \ldots$. The corresponding expression $u_m^0 = U_m(r,s)$ for $0 \leq m < 180$ satisfies $u_m^0 \equiv 0 \bmod p$ only when $m \in \{0, 1, 4, 6\}$. However, for these m one finds that u_m^1 is nonzero modulo p. Both lemmas of Skolem can be applied and it follows that there is no nontrivial symmetry except at order 6.

Almost integrable systems. We computed the resultant of U_n and U_m for $4 \leq n \leq 10$ and $n + 1 \leq m \leq n + 150$. To give an indication of the size of the expressions, the resultant of U_{10} and U_{160} has degree 556. In this polynomial, he coefficients of r^n with $244 < n < 312$ all have over 200 (decimal) digits. The number of n^{th} order systems we have calculated is

n	4	5	6	7	8	9	10	4–10
#	2745	2701	5679	5644	8740	8839	11952	46300

In the pictures on the next pages the positions of the roots of these resultants in the complex plane are plotted. As a fundamental domain the upper half unit circle is chosen. The full pictures are invariant under $r \mapsto \frac{1}{r}$ and $r \mapsto \bar{r}$.

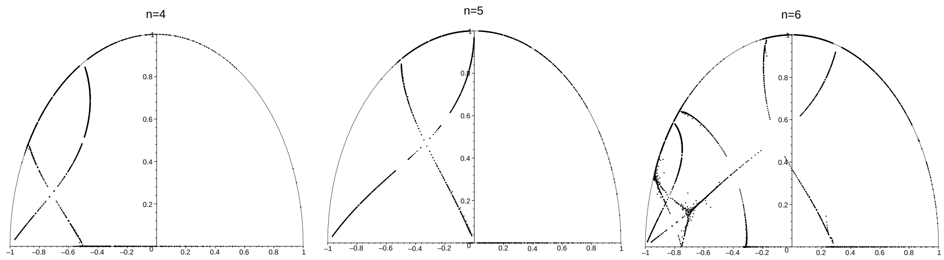

FIGURE 3. *Zeroes of the G–polynomials corresponding to almost integrable systems of order* $4, 5$ *and* 6.

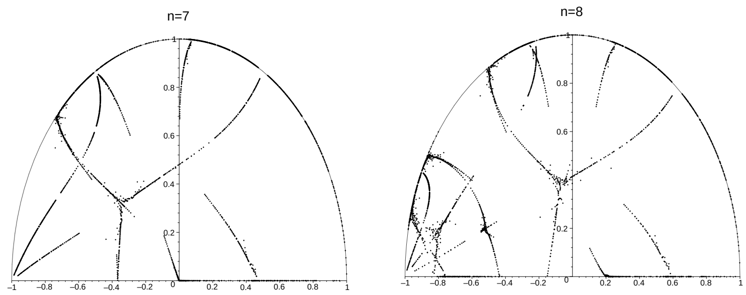

FIGURE 4. *Zeroes of the G–polynomials corresponding to almost integrable systems of order* 7 *and* 8.

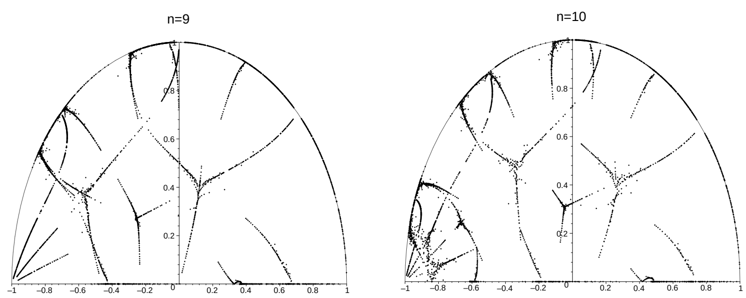

FIGURE 5. *Zeroes of the G–polynomials corresponding to almost integrable systems of order* 9 *and* 10.

All these systems have at least one nontrivial symmetry.

Refinement of the method of Skolem. To find the exact number of symmetries, we made the following refinements of the method of Skolem, which will be explained by means of examples.

Example: $n = 4, m = 11$. The resultant of $U_4(r, s)$ and $U_{11}(r, s)$ with respect to s contains the factor

$$f(r) = 3r^8 + 22r^7 + 69r^6 + 130r^5 + 159r^4 + 130r^3 + 69r^2 + 22r + 3.$$

With $p = 23$ we find $f(15) \equiv f(17) \equiv 0 \bmod p$, both corresponding to p-adic zeroes. With $0 \leq m < 22$ one finds $U_m(15, 17) = 0$ only if $m \in \{0, 1, 4, 11\}$. For these values of m the associated u_m^1 is not zero modulo p. The Skolem lemmas imply that the only non-trivial symmetry has order 11.

The fact that the degree of f is 8 indicates that there are two different 4th order systems with a symmetry of order 11. The argument given so far, shows the lack of other symmetries for only one of them. To prove it for the other system, it suffices to show that f is irreducible over $\mathbb{Q}$. This is the case, as follows, e.g., from the fact that $f(r)$ is irreducible modulo 31.

Example: $n = 4, m = 24$. Some resultants are irreducible, some are not. The resultant of $U_4(r, s)$ and $U_{24}(r, s)$ with respect to s contains the factors

$$11r^8 + 66r^7 + 183r^6 + 318r^5 + 379r^4 + 318r^3 + 183r^2 + 66r + 11$$

for which we can use Skolem's method with prime 131 (and $r = 15, s = 17$) and

$$17r^8 + 138r^7 + 427r^6 + 798r^5 + 969r^4 + 798r^3 + 427r^2 + 138r + 17$$

for which we can use Skolem's method with prime 877 (and $r = 10, s = 556$).

Example: $n = 5, m = 19$. The polynomial

$$\begin{aligned} f(r) = \; & r^{12} + 4r^{11} + 10r^{10} + 19r^9 + 28r^8 + 34r^7 \\ & + 37r^6 + 34r^5 + 28r^4 + 19r^3 + 10r^2 + 4r + 1 \end{aligned}$$

splits into distinct linear factors in $\mathbb{Z}_{509}[r]$. It is irreducible over $\mathbb{Q}$. Modulo $p = 509$, the pair $(264, 407)$ is a zero of $U_m(r, s) \bmod p$ when $m \in \{0, 1, 5, 19, 256, 414\}$. The pair $(267, 300)$ is a zero of $U_m(r, s) \bmod p$ when $m \in \{0, 1, 5, 19, 162, 254\}$. Using both pairs we can apply Skolem's first lemma for all $0 \leq m < 508$ except $\{0, 1, 5, 19\}$, and for these remaining values we could apply the second lemma. This method is quite successful here, since we could not find any prime (< 8124) for which the normal procedure works.

With these improvements of the p-adic method we have been able to prove

THEOREM 5.11. *Take* $3 < n < 11, n < m < n + 151$ *and* $m \neq 11, 29$ *when* $n = 7$. *Then all* n^{th} *order non-integrable* $\mathcal{B}$*-systems with a symmetry of order* m *are almost integrable of depth* 1.

Counterexamples to Fokas conjecture. The exceptional case in theorem 5.11 disproves a conjecture made in [**Fok87**], where Fokas suggested that if a scalar equation possesses at least one time-independent non-Lie point symmetry, then it possesses infinitely many. Similarly for n-component equations one needs n symmetries.

Counterexample [**vdKS99, vdKS01**]: take $n = 7, m = 11, 29$. The resultant of $U_7(r, s)$ and $U_{11}(r, s)$ with respect to s as well as the resultant of $U_7(r, s)$ and $U_{29}(r, s)$ with respect to s contains the factors

$$(r^3 + r^2 - 1)(r^3 - r - 1)(r^6 + 3r^5 + 5r^4 + 5r^3 + 5r^2 + 3r + 1).$$

In $\mathbb{Z}/101\mathbb{Z}$, the second factor has the zero 20 and the third one 52. These can be lifted to zeroes in $\mathbb{Z}_{101}$ and Skolem's lemmas can be applied. We do not have to worry about the first factor because its degree is smaller than 4 (indeed, it has a zero $\frac{1}{20} \bmod 101 \equiv 96$).

5.4. Second order two dimensional equations. A classification of integrable second order two dimensional equations is to be found in [**SW01**]. Part of the analysis is reviewed here to illustrate the techniques involved. Suppose that $K^{-1,1}$ is not zero and the second component of $K^{1,0}$ is nonzero as well. This is for example the case in

$$\begin{aligned} u_t &= au_2 + v^2 \\ v_t &= v_2 + uv. \end{aligned}$$

A symmetry of such a system has the form

$$\begin{aligned} u_t &= bu_m + \cdots \\ v_t &= v_m + \cdots \end{aligned}$$

Then (assuming integrability) there is the following branch. There should be infinitely many m such that

$$b = \frac{\alpha^m + 1}{(\alpha + 1)^m} = (\frac{a+1}{2})^m - (\frac{a-1}{2})^m,$$

where

$$a = (\alpha^2 + 1)/(\alpha + 1)^2.$$

When $a \neq -1, 1$, we apply the theorem of Lech and Mahler to see that the ratios

$$\frac{2\alpha}{(\alpha+1)(a+1)}, \frac{2}{(\alpha+1)(a-1)}$$

are roots of unity. The condition $|\frac{2\alpha}{(\alpha+1)(a+1)}| = 1$ implies

$$|\alpha(\alpha+1)| = |\alpha^2+\alpha+1|,$$

i.e., $\Re\left(\alpha(\alpha+1)\right) = -\frac{1}{2}$. The condition

$$|\frac{2}{(\alpha+1)(a-1)}| = 1$$

implies $|\alpha| = |\alpha+1|$, i.e., $\Re\alpha = -\frac{1}{2}$. Together these imply $\alpha = -\frac{1}{2} \mp \frac{i}{2}$. Then $a = -1 \pm 2i$. Since a is invariant under $\alpha \mapsto \frac{1}{\alpha}$ the second pair gives the same values for a. We define

$$\Delta(\alpha, m) = (\frac{a+1}{2})^m - (\frac{a-1}{2})^m - \frac{\alpha^m+1}{(\alpha+1)^m}$$

where $\alpha = -\frac{1}{2} \mp \frac{i}{2}$. Its value only depends on a since $\Delta(\frac{1}{\alpha}, m) = \Delta(\alpha, m)$. Notice that $\Delta(\alpha, m) = 0$ if and only if

$$0 = (\frac{1}{2})^m - (-\frac{1}{2})^m - 2(\frac{\sqrt{2}}{2})^m \cos\frac{m\pi}{4}.$$

Solving this, we obtain

$$m \equiv 2 \mod 4$$

or

$$m = 1.$$

It follows that $b = i^m \mp (1-i)^m$ when

$$a = -1 \pm 2i.$$

Following similar reasoning all possible eigenvalues and orders of possible symmetries are obtained for all possible combinations λ_1, λ_2. Finally the implicit function theorem is used to prove integrability of the systems involved.

6. Conclusion

The application of number theory in the analysis of integrable systems is quite successful and promising. It is another unexpected application of pure mathematics and it illustrates the need of communication among the different branches of mathematics and mathematical physics.

Bibliography

[Bak91] I. M. Bakirov. On the symmetries of some system of evolution equations. Technical report, Akad. Nauk SSSR Ural. Otdel. Bashkir. Nauchn. Tsentr, Ufa, 1991.

[Beu97] Frits Beukers. On a sequence of polynomials. *J. Pure Appl. Algebra*, 117/118:97–103, 1997.

[BS01] Frits Beukers and Chris J. Smyth. Cyclotomic points on curves. In *Millennial Conference on Number Theory, May 21-26, 2000, Urbana-Champaign*. AK Peters, 2001.

[BSW98] Frits Beukers, Jan A. Sanders, and Jing Ping Wang. One symmetry does not imply integrability. *J. Differential Equations*, 146(1):251–260, 1998.

[BSW01] Frits Beukers, Jan A. Sanders, and Jing Ping Wang. On integrability of systems of evolution equations. *J. Differential Equations*, 172(2):396–408, 2001.

[Fok80] A. S. Fokas. A symmetry approach to exactly solvable evolution equations. *J. Math. Phys.*, 21(6):1318–1325, 1980.

[Fok87] A. S. Fokas. Symmetries and integrability. *Studies in Applied Mathematics*, 77:253–299, 1987.

[Fou00] Mikhail V. Foursov. On integrable coupled KdV-type systems. *Inverse Problems*, 16(1):259–274, 2000.

[Gar71] Clifford S. Gardner. Korteweg-de Vries equation and generalizations. IV. The Korteweg-de Vries equation as a Hamiltonian system. *J. Math. Phys.*, 12:1548–1551, 1971.

[GGKM74] Clifford S. Gardner, John M. Greene, Martin D.Kruskal, and Robert M. Miura. Korteweg-deVries equation and generalization. VI. Methods for exact solution. *Comm. Pure Appl. Math.*, 27:97–133, 1974.

[Ger93] Vladimir P. Gerdt. Computer algebra, symmetry analysis and integrability of nonlinear evolution equations. *Internat. J. Modern Phys. C*, 4(2):279–286, 1993.

[Ger96] V. P. Gerdt. Homogeneity of integrability conditions for multi-parametric families of polynomial–non-linear evolution equations. *Math. Comput. Simulation*, 42(4-6):399–408, 1996. Symbolic computation, new trends and developments (Lille, 1993).

[GD75] I.M. Gel'fand and L.A. Dikiĭ. Asymptotic properties of the resolvent of Sturm-Liouville equations, and the algebra of Korteweg-de Vries equations. *Russian Math. Surveys*, 30 (1975), no. 5, 77–113.

[GKZ90] V. P. Gerdt, N. A. Kostov, and A. Yu. Zharkov. Nonlinear evolution equations and solving algebraic systems: the importance of computer algebra. In *Solitons and applications (Dubna, 1989)*, pages 120–128. World Sci. Publishing, River Edge, NJ, 1990.

[Gou97] Fernando Q. Gouvêa. *p-adic numbers*. Springer-Verlag, Berlin, second edition, 1997.

[IŠ80] N. H. Ibragimov and A. B. Šabat. Evolution equations with a nontrivial Lie-Bäcklund group. *Funktsional. Anal. i Prilozhen.*, 14(1):25–36, 96, 1980.

[KdV95] D. J. Korteweg and G. de Vries. On the change of form of long waves advancing in a rectangular canal, and a new type of long stationary waves. *Philos. Mag.*, 39(5):422–443, 1895.

[KMGZ70] Martin D. Kruskal, Robert M. Miura, Clifford S. Gardner, and Norman J. Zabusky. Korteweg-de Vries equation and generalizations. V. Uniqueness and nonexistence of polynomial conservation laws. *J. Mathematical Phys.*, 11:952–960, 1970.

[Lec53] C. Lech. A note on recurring sequences. *Arkiv. Mat.*, 2:417–421, 1953.

[Mag78] F. Magri. A simple model of integrable Hamiltonian equation. *J. Math. Phys.*, 19(5):1156–1162, 1978.

[MGK68] Robert M. Miura, Clifford S. Gardner, and Martin D. Kruskal. Korteweg-de Vries equation and generalizations. II. Existence of conservation laws and constants of motion. *J. Math. Phys.*, 9:1204–1209, 1968.

[Miu68] Robert M. Miura. Korteweg-de Vries equation and generalizations. I. A remarkable explicit nonlinear transformation. *J. Math. Phys.*, 9:1202–1204, 1968.

[MŠS91] A. V. Mikhaĭlov, A. B. Šabat, and V. V. Sokolov. The symmetry approach to classification of integrable equations. In *What is integrability?*, Springer Ser. Nonlinear Dynamics, pages 115–184. Springer-Verlag, Berlin, 1991.

[Olv93] Peter J. Olver. *Applications of Lie groups to differential equations*, volume 107 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1993.

[OS98] Peter J. Olver and Vladimir V. Sokolov. Integrable evolution equations on associative algebras. *Comm. Math. Phys.*, 193(2):245–268, 1998.

[OW00] Peter J. Olver and Jing Ping Wang. Classification of integrable one-component systems on associative algebras. *Proc. London Math. Soc. (3)*, 81(3):566–586, 2000.

[SG69] C. H. Su and C. S. Gardner. Korteweg-de Vries equation and generalizations. III. Derivation of the Korteweg-de Vries equation and Burgers equation. *J. Math. Phys.*, 10:536–539, 1969.

[SW98] Jan A. Sanders and Jing Ping Wang. On the integrability of homogeneous scalar evolution equations. *J. Differential Equations*, 147(2):410–434, 1998.

[SW00] Jan A. Sanders and Jing Ping Wang. On the integrability of non-polynomial scalar evolution equations. *J. Differential Equations*, 166(1):132–150, 2000.

[SW01] J.A. Sanders and J.P. Wang. On the integrability of systems of second order evolution equations with two components. Technical Report WS–557, Vrije Universiteit Amsterdam, Amsterdam, 2001. Submitted to Journal of Differential Equations.

[vdK02] Peter H. van der Kamp. On proving integrability. *Inverse Problems*, 18:405–414, 2002.

[vdKS99] P.H. van der Kamp and J.A. Sanders. Almost integrable evolution equations. Technical Report WS–534, Vrije Universiteit Amsterdam, 1999. To be published in Selecta Mathematica.

[vdKS01] P.H. van der Kamp and J.A. Sanders. On testing integrability. *J. Nonlinear Math. Phys.*, 8(4):561–574, 2001.

[Wan98] J.P. Wang. *Symmetries and Conservation Laws of Evolution Equations*. PhD thesis, Vrije Universiteit, Amsterdam, 1998.

[Zak91] V.E. Zakharov, editor. *What is Integrability?* Springer–Verlag, Berlin, 1991.